TechXplore

No honor among cyber thieves

July 22 2020, by Will Ferguson

Alex Kigerl, Washington State University Credit: WSU

A backstabbing crime boss and thousands of people looking for free tutorials on hacking and identity theft were two of the more interesting findings of a study examining user activity on two online 'carding forums,' illegal sites that specialize in stolen credit card information.

As instances of online identity theft continue to rise over the course of the coronavirus pandemic, the research helps shed light on the shady world of cybercriminals and how it operates.

"The cybercrime marketplace, like most e-commerce, has continued to expand and carding forums are the most widespread formats in the West for exchanging illicit goods," said Alex Kigerl, a Washington State University criminologist and lead author of the study published in the June edition of *Social Science Computer Review*.

For the study, Kigerl used hacked and leaked data from the two online marketplaces where credit card information is bought and sold to reveal the activity patterns and messages of some 10,714 of the sites' users.

His analysis of data from the two carding forums revealed the vast majority of users weren't there to buy or sell anything but rather wanted free samples of credentialed goods, malware source codes, and tutorials on hacking and identify theft.

Actual buyers and sellers of stolen information comprised only a fraction of the total user base of the two websites, Fraud and Elitecarders.

These users were primarily buying and selling stolen identity information that enables them to make unauthorized online purchases, set up a bank account in another person's name or even create a clone of a victim's credit card that can be used in physical retail shops.

Kigerl also discovered that the administrator of the two carding forums, the person who is typically in charge of vouching for reputable sellers and banning users who defraud other users, was perhaps the biggest thief of all.

The administrator would offer up fake credit card information and then ban users who purchased it to keep them from reporting the fraud to the public forums.

"This was very unusual behavior because it is generally in the interest of an administrator to promote good interactions so that he or she can make money from offering things like escrow services," Kigerl said. "It just goes to show there really is no honor among thieves."

A growing online black market

Cybercrime, like most e-commerce, has continued to expand throughout the course of the coronavirus pandemic. In June, the FBI reported an almost 75% spike in daily cybercrimes since the start of stay at home restrictions.

Kigerl said the illicit online marketplaces where most of this criminal activity takes place generally fall into one of four categories—internet relay chat, carding shops, darknet marketplaces and carding forums.

By far the most popular, carding forums are easier to access than other cybercrime marketplaces because they are hosted on the regular internet rather than the dark web, which requires a special internet protocol to access.

They consist of multiple boards pertaining to specialized topics such as credit card sellers, malware distribution, and free tutorials. Users must register a profile with the website to be able to comment.

Profiles can then be used to track trustworthiness ratings, and each board has one or more moderators who can act as a sort of law enforcement agent, banning disruptive members and setting guidelines.

Carding forums also typically have a short shelf life, only lasting for a few months before being taken down by law enforcement.

"It is kind of like whack-a-mole," Kigerl said. "One of these websites will go down, and the community will just create a new site and start the process over again. Unfortunately, due to issues of jurisdiction and technologically sophisticated ways to hide one's identity online, few of these criminals get apprehended."

Kigerl said that developing a better understanding of how users operate on carding forums and other cybercrime marketplaces could ultimately help to both apprehend criminals and keep regular internet users safe.

"The more time we spend online, the more we risk exposing our personal information to cybercriminals," Kigerl said. "Other than the usual, such as keeping your computer updated, installing AV software and using a spam filter, I recommend using a service like virustotal.com when you encounter a suspicious file or URL. It scans the file or link with dozens of separate antivirus programs and automatically shares any issues with the security community."

More information: Alex Kigerl, Behind the Scenes of the Underworld: Hierarchical Clustering of Two Leaked Carding Forum Databases, *Social Science Computer Review* (2020). DOI: 10.1177/0894439320924735

Provided by Washington State University

Citation: No honor among cyber thieves (2020, July 22) retrieved 10 April 2024 from https://techxplore.com/news/2020-07-honor-cyber-thieves.html