Prevention better than cure at preventing young users from getting involved in cybercrime

October 21 2019

Credit: CC0 Public Domain

Highly-targeted messaging campaigns from law enforcement can be surprisingly effective at dissuading young gamers from getting involved in cybercrime, a new study has suggested.

The study, by researchers from the University of Cambridge and University of Strathclyde, looked at four different types of law enforcement interventions, the first evaluation of the their effectiveness for this particular type of cybercrime.

They found that while high-profile arrests and sentencing of cybercriminals only lead to a short drop in the number of attacks taking place, the takedown of infrastructure and targeted messaging campaigns were strongly associated with a sharper and longer-term reduction in attack numbers. The results will be presented today (21 October) at the ACM Internet Measurement Conference in Amsterdam.

For just a few dollars, almost anyone can become involved in cybercrime through the use of 'booter' service websites, where users can purchase targeted denial of service (DoS) attacks. A DoS attack generates large amounts of traffic which overwhelm end users or web services, taking them offline.

DoS attacks have been used in the past as a protest tactic, but because of booter services and the relative ease of using them, they are commonly used by users of gaming sites, as a form of retaliation against other users—the largest booter provider carries out between 30,000 and 50,000 such attacks every day.

While DoS attacks are usually targeted at a specific end users, they can often cause collateral damage, knocking out other users or systems.

"Law enforcement are concerned that DoS attacks purchased from a booter site might be like a 'gateway drug' to more serious cybercrime,"

said Ben Collier from Cambridge's Department of Computer Science & Technology, the paper's first author. "A big problem is that there is still relatively little evidence as to what best practice looks like for tackling cybercrime."

"Even people running booter services think that booting is lame," said Dr. Daniel Thomas from Strathclyde's Department of Computer and Information Sciences. "This makes the market particularly vulnerable to disruption."

Collier and his colleagues from the Cambridge Cybercrime Centre used two datasets with granular data about the attacks from booter sites, and modelled how the data correlated with different intervention tactics from the National Crime Agency (NCA) in the UK, the Federal Bureau of Investigation (FBI) in the US, and other international law enforcement agencies.

While operating a booter service or purchasing a DoS attack is illegal in most jurisdictions, earlier research has found that most booter operators were unconcerned about the possibility of police action against them.

The researchers found that arrests only had a short-term effects on the volume of DoS attacks—about two weeks—at which point activity went back to normal. Sentencing had no widespread effect, as attackers in one country weren't affected by sentences in another country.

Taking down infrastructure—as the FBI did at the end of 2018—had a far more noticeable effect, and suppressed the booter market for months. "This FBI action also reshaped the market: before, it was what you'd expect in a mature ecosystem, where there several large booter services and lots of smaller ones," said Collier. "But now there's really just one large booter service provider, and you're starting to see a few smaller ones start to come back."

The most interesting results were around targeted messaging. From late December 2017 to June 2018, the NCA bought targeted Google adverts aimed at young men in the UK. When a user searched for booter services, a targeted advert popped up, explaining that DoS attacks are illegal.

"It's surprising, but it seems to work, like a type of digital guardianship," said Collier. "At the exact moment you get curious about getting involved in cybercrime, you get a little tap on the shoulder.

"It might not work for people who are already involved in this type of cybercrime, but it appeared to dramatically decrease the numbers of new people getting involved."

While the researchers say this evidence suggests that targeted online messaging has the potential to be a potent tool for preventing crime, it also poses questions about what accountability structures might be required for its wider use as a police tactic.

This has already had direct policy impact, and the FBI and NCA have used this research to inform their strategies for dealing with booter services.

Provided by University of Cambridge