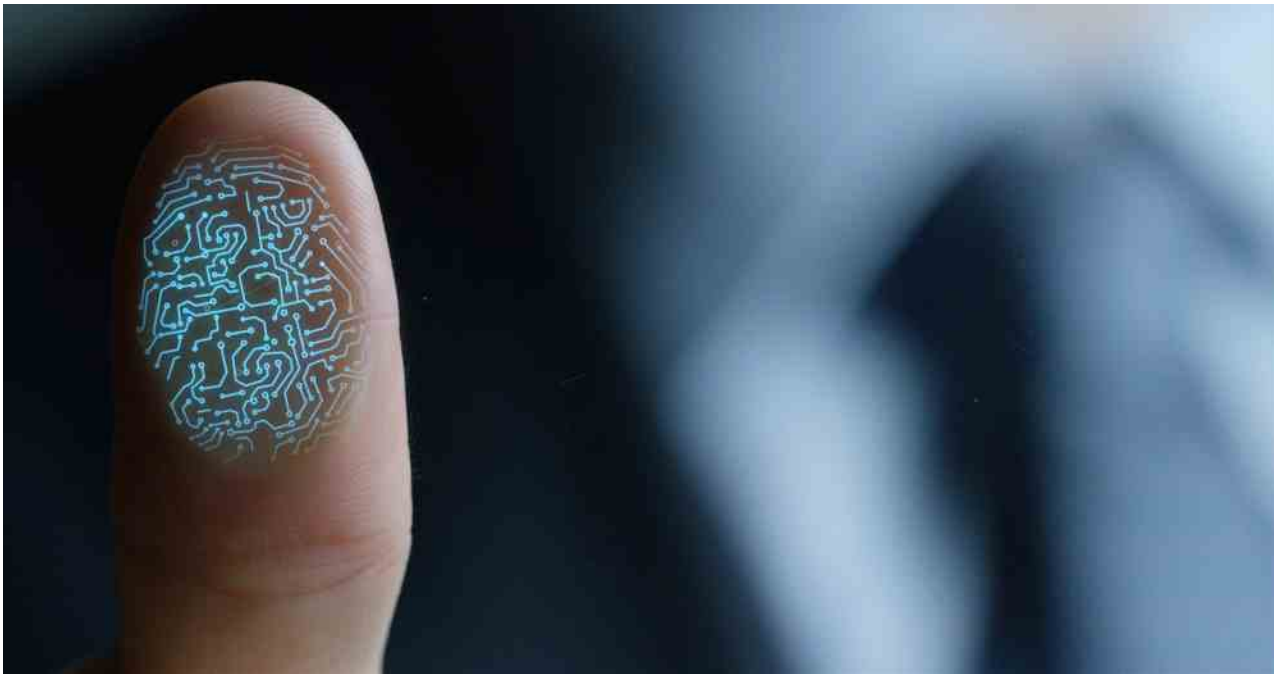
Criminaliteitspatronen van hackers die websites ‘defacen’

nscr.nl/criminaliteitspatronen-van-hackers-bij-website-defacements

29 september 2021

Cybercrime is de afgelopen decennia snel toegenomen in omvang. Hacking is zelfs de meest voorkomende vorm van criminaliteit in Nederland. Maar het is onbekend of bevindingen over traditionele daders ook gelden voor cybercriminelen. Wetenschappers van het NSCR onderzochten daarom of hackers die websites ‘defacen’ vergelijkbare longitudinale criminaliteitspatronen volgen als traditionele daders. Daarnaast keken ze of aannames over herhaald slachtofferschap ook gelden voor website-defacements.

Door dr. Asier Moneva; dr. Steve van de Weijer; dr. Rutger Leukfeldt | 29 september 2021 | Cybercrime



Dit artikel is alleen beschikbaar in het Engels.
Previous studies have shown that traditional (offline) types of crime concentrate strongly within offenders, as a small group of chronic offenders is responsible for the majority of offenses. The rest of the offenders tend to have a short criminal career in which they only commit a few crimes often during adolescence or early adulthood. Whether cyber offenders follow similar offending patterns remained unknown because of a lack of longitudinal panel studies that measure self-reported involvement in cybercrime and the low number of convictions in judicial data.

Outlet for hackers to publicly report defaced websites

In three recent publications, NSCR researchers used unique data from the archive of web defacements 'Zone-H'. During a web defacement, hacking techniques are used to change the content of an active website to a set of images, text, and sound files selected by the attacker. Zone-H provides an outlet for hackers who engage in web defacements to publicly report websites that they have defaced. When reporting to Zone-H, hackers are asked to provide a hacker handle (i.e., an adopted online identity of the individual or group), which was used to identify which hackers or hacker groups were responsible for each web defacement.

Most hackers only performed web defacements during a limited time period

NSCR researchers Steve van de Weijer and Rutger Leukfeldt collaborated with professor Thomas Holt from Michigan State University to examine the longitudinal offending patterns of 66,553 hackers who reported 2.7 million web defacement attacks to Zone-H, between January 2010 and March 2017. They identified six different groups with different offending patterns. A small group of *high chronic* offenders (2.9% of all web defacers) defaced websites at high rate throughout the research period and was responsible for more than two thirds (68.5%) of all defacements reported to Zone-H. This degree of concentration within chronic cyber offenders is even stronger than in most studies among traditional offenders. Moreover, most hackers only performed one or a few web defacements during a limited time period, which aligns with offending patterns that are observed among most traditional offenders.

To be the best defacer

The motivations, hacking methods, and selected targets were also compared between the six groups of web defacers with different offending patterns. This showed, for example, that the *high chronic* offenders relatively often defaced websites because they 'want to be the best defacers' and that they are less likely to deface homepages of websites compared to the other groups. In a related study, Van de Weijer, Leukfeldt, and Holt performed the same analyses among a sub sample of web defacements directed at Dutch websites (with a .nl extension), which led to similar results.

Strengthening cyber security measures after an initial incident

In a third study, NSCR researchers Asier Moneva, Rutger Leukfeldt, and Steve Van de Weijer, together with professor Fernando Miro from Miguel Hernandez University, used over 9 million records from Zone-H to examine patterns of repeat victimisation. They examined whether – in line with previous studies on repeat victimisation by traditional crime – high crime rates were the result of repeat victimisation; repeats tended to recur quickly; repeats were mainly caused by prolific offenders; and offenders repeatedly victimise previous targets. The results showed similarities and discrepancies between traditional offending and cyber offending. For example, data showed that repeated defacements accounted for about 7% of all hacks and contributed little to the annual

variation in incidents. Nevertheless, some website domains were repeatedly targeted over the course of up to seven years, which reflects the importance of strengthening the cyber security measures after an initial incident.

Very high crime concentration among offenders

In line with the abovementioned studies, researchers found that most defacers carried out few attacks, but that few defacers carried out repeated attacks. In particular, 1% of the re-defacers committed about 58% of the repeats, and 50% of them committed about 98%. This is again a sign of a very high crime concentration among offenders. It should be noted though that defacers rarely targeted again the same websites that they had previously hacked – this only occurred in 0.3% of the time. In fact, only about 6% of repeats was due to the same offenders defacing the same websites repeatedly. For context, researchers point out that Zone-H data probably underestimate the share of repeats in website defacements. So, it is likely that actual figures are much higher.

Invaluable information for cybercrime prevention

These studies focus on the barely explored dimension of cyber offending using a unique data source. The results contribute to understanding how and why website defacements are concentrated in a few individuals and locations. Identifying the most prolific defacers and understanding their criminal patterns provides invaluable information for cybercrime prevention, especially given the economic, political, and reputational impact these attacks can cause. If a few cyber offenders commit the majority of attacks, focusing preventive resources on them can substantially reduce or mitigate the impact of their attacks.

Publication details and further reading

Leukfeldt, R. & Holt, T. (2021). Cybercrime on the menu? Examining cafeteria-style offending among financially motivated cybercriminals. *Computers in Human Behavior.*
Van de Weijer, S., Leukfeldt, R. & Holt, T. (2021). Ontwikkelingstrajecten van hackers: een longitudinale studie naar defacements op Nederlandse websites. *Tijdschrift voor Veiligheid.*
Moneva, A., Leukfeldt, R., Van de Weijer, S. & Miró-Llinares, F. (2021). Repeat victimization by website defacement: An empirical test of premises from an environmental criminology perspective. *Computers in Human Behavior.*