Researchers find huge, sophisticated black market for trade in online 'fingerprints'

23 October 2020

Credit: CC0 Public Domain

Security on the internet is a never-ending cat-and-mouse game. Security specialists constantly come up with new ways of protecting our treasured data, only for cyber criminals to devise new and crafty ways of undermining these defenses. Researchers at TU/e have now found evidence of a highly sophisticated Russian-based online marketplace that trades hundreds of thousands of very detailed user profiles. These personal 'fingerprints' allow criminals to circumvent state-of-the-art authentication systems, giving them access to valuable user information, such as credit card details.

Our online economy depends on usernames and passwords to make sure that the person buying stuff or transferring money on the internet, is really the person they are saying. However, this limited way of authentication has proven to be far from secure, as people tend to reuse their passwords across several services and websites. This has led to a massive and highly profitable illegal trade in user credentials: According to a recent estimate (from 2017) some 1.9 billion stolen identities were sold through underground markets in a year's time.

It will come as no surprise that banks and other digital services have come up with more complex authentication systems, which rely not only on something the users know (their password), but also something they have (e.g. a token). This process, known as multi-factor authentication (MFA), severely limits the potential for cybercrime, but has drawbacks. Because it adds an extra step, many users don't bother to register for it, which means that only a minority of people use it.

To alleviate this problem, an alternative system of authentication has recently become popular with services such as Amazon, Facebook, Google and PayPal. This system, known as Risk-based Authentication (RBA), looks at 'user fingerprints' to check someone's credentials. These can include basic technical information, such as type of browser or operating system, but also behavioral features, such as mouse movement, location and keystroke speed. If the fingerprint complies with what is expected from a user—based on earlier behavior—they are allowed to login right away, using only their usernames and passwords. If not, additional authentication through a token is required.

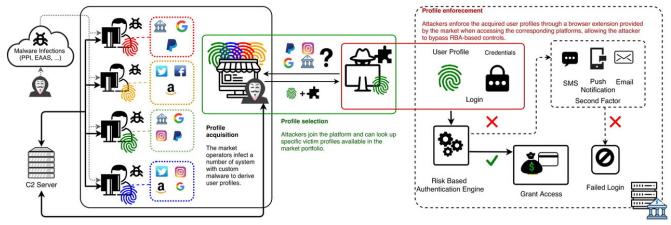
Of course, cyber criminals have quickly come up with ways of circumventing RBA, developing phishing kits that also include fingerprints. However, they have found it hard to turn this in an effective and profitable business. One of the reasons is that these user profiles vary with time and across services and must be collected through additional phishing attacks.

Impersonation-as-a-service

Researchers at TU/e have now found evidence of a largescale and highly sophisticated marketplace that appears to overcome these limits. The marketplace, which is based in Russia, offers more than 260.000 highly detailed user profiles, together with other user credentials, such as email

addresses and passwords. "What is unique about this underground website is not only its scale, but also the fact that all the profiles are continually updated, which means they retain their value," says Luca Allodi, researcher at the Security group at the department of Mathematics and Computer Science, who together with Ph.D. student Michele Campobasso was responsible for the research.

"In addition, customers can search the database, so that they select precisely the internet user they want to target, enabling highly dangerous spearphishing attacks. They can also download software that automatically loads the purchased user profiles in the targeted websites."



Credit: Eindhoven University of Technology

To stress the systematic nature of the website, Allodi and Campobasso have coined the term 'Impersonation-as-a-service' (IMPaaS), echoing well-known cloud-computing services like SaaS (software-as-a-service) and IaaS (infrastructure-as-a-service). "As far as we know this is the largest and most sophisticated criminal marketplace to systematically offer these services."

Researching the marketplace wasn't easy. To get access to the listings of available user profiles, the researchers had to get hold of special invite codes shared by existing users. Harvesting the data was also difficult, as the platform operators actively monitor 'rogue' accounts. The researchers have also decided to keep secret the real name of the website to minimize the risk of retaliatory actions from the market operators.

Price

The price of a user's 'virtual identity' on the marketplace ranges from 1 dollar to approximately 100 dollar. Access to cryptocurrency profiles and webmoney platforms seem to be the most valued. "The mere presence of at least one crypto-related profile nearly doubles the average profile value," says Allodi.

Another important factor driving up the price is the wealth of the country where the user is located. "This makes sense: attackers looking to impersonate and monetize user profiles assign a greater value to profiles that are likely to bring larger financial gains, and these are mainly found in developed countries," according to Campobasso.

Also very highly valued are user profiles that give access to more than one service and profiles with 'real' fingerprints, as opposed to fingerprints 'synthesized' by the platform.

Putting the profiles to use

In their paper the researchers also describe a few examples of how criminals 'weaponize' these profiles, which they found on a secret Telegram channel used by platform clients. In one of the reported attacks, an attacker describes setting filters to a victim's email mailboxes, with the aim of hiding notifications from Amazon related to purchases the attacker made using the victim's Amazon account.

More information: Michele Campobasso, Luca Allodi. Impersonation-as-a-Service: Characterizing the Emerging Criminal Infrastructure for User Impersonation at Scale. arXiv:2009.04344 [cs.CR]
DOI: 10.1145/3372297.3417892
arxiv.org/abs/2009.04344

Provided by Eindhoven University of Technology