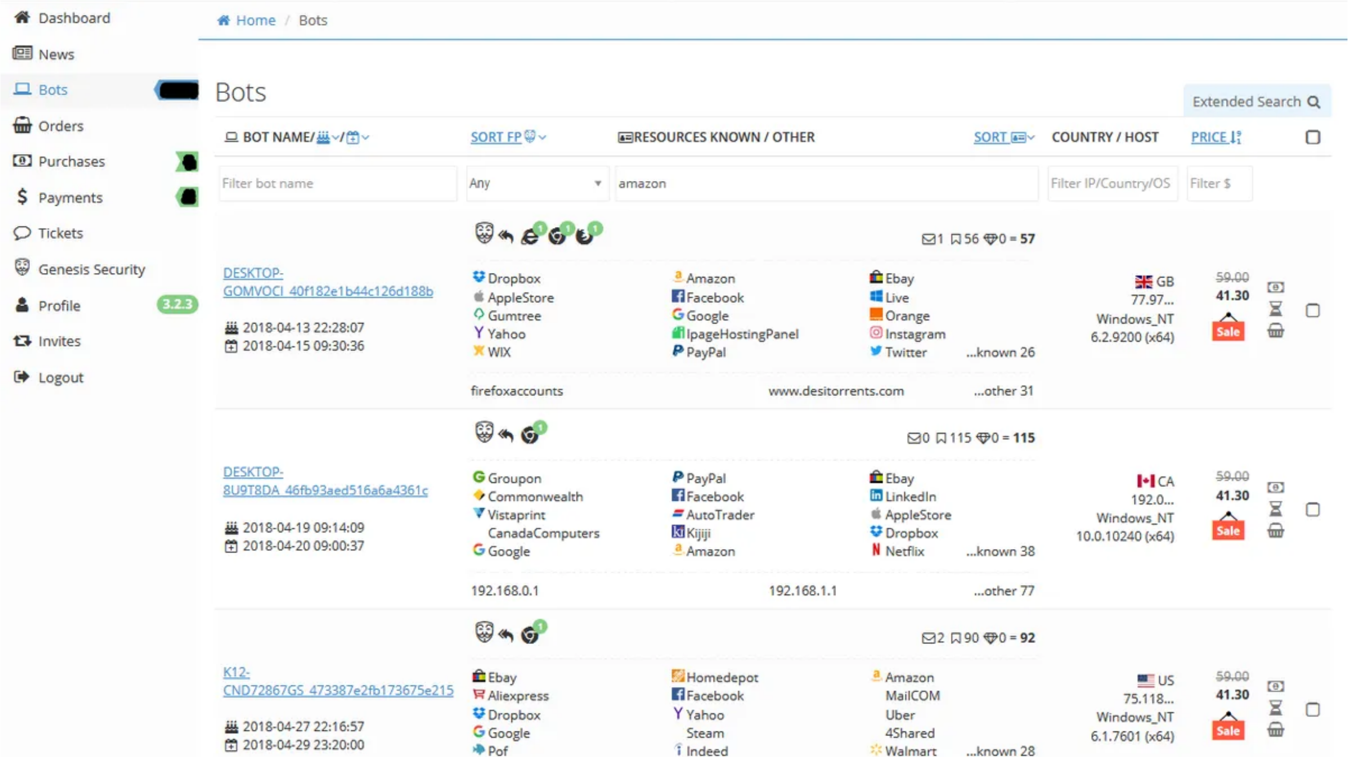
Cybercrime market selling full digital fingerprints of over 60,000 users

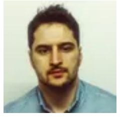
zdnet.com/article/cybercrime-market-selling-full-digital-fingerprints-of-over-60000-users/



BOT NAME/	SORT FP	RESOURCES KNOWN / OTHER	SORT	COUNTRY / HOST	PRICE	□
Filter bot name	Any ▾	amazon		Filter IP/Country/OS	Filter $	
DESKTOP-GOMVOCI_40f182e1b44c126d188b 2018-04-13 22:28:07 2018-04-15 09:30:36		✉1 🔖56 💎0 = **57** Dropbox, AppleStore, Gumtree, Yahoo, WIX Amazon, Facebook, Google, IpageHostingPanel, PayPal Ebay, Live, Orange, Instagram, Twitter ...known 26 firefoxaccounts www.desitorrents.com ...other 31		GB 77.97... Windows_NT 6.2.9200 (x64)	~~59.00~~ **41.30** Sale	□
DESKTOP-8U9T8DA_46fb93aed516a6a4361c 2018-04-19 09:14:09 2018-04-20 09:00:37		✉0 🔖115 💎0 = **115** Groupon, Commonwealth, Vistaprint, CanadaComputers, Google PayPal, Facebook, AutoTrader, Kijiji, Amazon Ebay, LinkedIn, AppleStore, Dropbox, Netflix ...known 38 192.168.0.1 192.168.1.1 ...other 77		CA 192.0... Windows_NT 10.0.10240 (x64)	~~59.00~~ **41.30** Sale	□
K12-CND72867GS_473387e2fb173675e215 2018-04-27 22:16:57 2018-04-29 23:20:00		✉2 🔖90 💎0 = **92** Ebay, Aliexpress, Dropbox, Google, Pof Homedepot, Facebook, Yahoo, Steam, Indeed Amazon, MailCOM, Uber, 4Shared, Walmart ...known 28		US 75.118... Windows_NT 6.1.7601 (x64)	~~59.00~~ **41.30** Sale	□

Home Innovation Security

Genesis service is selling users' personal data, complete with digital fingerprints, such as account credentials, cookies, browser user-agent details, and more.



Written by Catalin Cimpanu, Contributor on April 9, 2019

-
-
-
-
-

Today, at the Kaspersky Security Analyst Summit conference taking place in Singapore, security researchers from Kaspersky Lab have revealed the existence of a new cybercrime marketplace where crooks are selling full digital fingerprints for over 60,000 users.

This new marketplace is like nothing that has ever been seen on the hacking scene until now.

Named Genesis, the service launched in the fall of 2018, when its creators began advertising it as a "secondary/related service" on several carding forums (forums where cyber-criminals sell stolen payment card details).

Genesis ad

Image: ZDNet

Genesis' main product is users' full digital profiles.

Users who in the past have been infected with malware or who have installed rogue browser extensions have unknowingly had their account passwords and full browser details recorded, and then sent to Genesis operators.

Each user profile includes login credentials for accounts on online payment portals, e-banking services, file-sharing or social networking services, but also the cookies associated with those accounts, browser user-agent details, WebGL signatures, HTML5 canvas fingerints, and other browser and PC details.

Genesis operators make their profits by selling this information on their marketplace to other cyber-criminal groups. The marketplace's main clientele are cyber-criminal engaged in online fraud, identity theft, and money mule operations.

Genesis buyers can acquire a user's digital identity for prices ranging from $5 to $200 and then log into that user's account to steal funds, personal photos, sensitive or proprietary documents, or submit official papers on his behalf (to government-related agencies).

Genesis marketplace

Image: ZDNet

To use any of the user identities crooks buy from Genesis, buyers will have to install a Chrome extension that has been created by the Genesis team.

This extension, provided free of charge to any buyer, automatically imports and applies a Genesis-bought identity, transforming the buyer's browser into a near-identical clone of the real user's browser.

Genesis extension

Image: ZDNet

The reason why a marketplace like Genesis has come to exist today is because in recent years, online services have improved their anti-fraud systems, and are now capable of detecting abnormal account login activity by looking at more details, rather than only a user's username and password.

Genesis identities (also called masks or fingerprints) will allow a crook to look as close to the real account owner as possible, fooling some of these modern anti-fraud systems, often deployed with online payment and e-banking services.

In an online ad found by ZDNet, Genesis' creators claim they "reviewed top 47 analytical systems and 283 major banks and payment systems" in order to determine what tracking and detection systems their cloned fingerprints needed to bypass.

Genesis details

Image: ZDNet

Kaspersky said today that Genesis has already entered the arsenal of some cyber-criminal gangs, and they are "actively using such digital doppelgangers to bypass advanced anti-fraud measures."

Experts recommend that users enable multing-factor authentication for every online account that supports it, but also recommend that companies add support for additional user identification mechanisms, such as biometrics.

A basic guide to diving in to the dark web

Related malware and cybercrime coverage: