Malware group leaks millions of stolen authentication cookies

therecord.media/malware-group-leaks-millions-of-stolen-authentication-cookies/

May 5, 2021

To add insult to injury, after users were infected by a malware strain that stole their passwords and personal data, the malware operators forgot to secure their backend servers, which leaked sensitive user information for hundreds of thousands of victims for more than a month.

For weeks, Bob Diachenko, Cyber Threat Intelligence Director at security firm Security Discovery, has been trying to convince a cloud provider to intervene and take down a malware group's server that was leaking **hundreds of thousands of stolen passwords** and **millions of authentication cookies**.

The data was leaked via an Elasticsearch server left exposed online without a password.

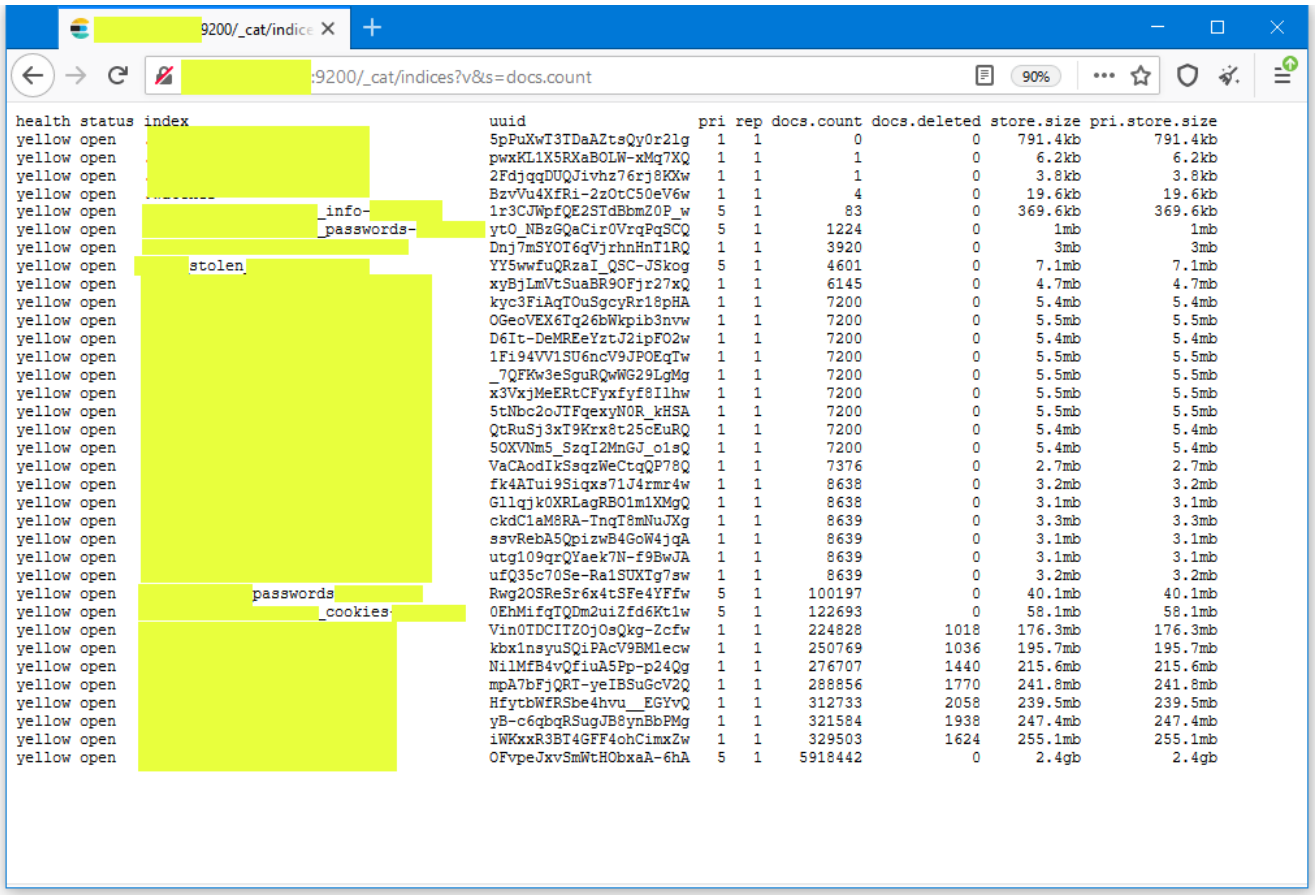

Image: The Record

The server exposed data that is typically collected by a type of malware known as an infostealer. This type of malware infects devices and then collects user credentials from web browsers, FTP, and email clients, data that is later uploaded to command and control (C&C) servers.

Typically, most C&C servers are hosted on a hacked website or a cheap virtual private server (VPS), and then the data is aggregated in a so-called data lake, where it is centralized for further analysis.

The Elasitcsearch server discovered by Diachenko is believed to be one of these data lakes, where crooks were aggregating their stolen information.

According to Vitali Kremez, CEO of threat intelligence company Advanced Intelligence, and James Maude, lead cyber-security researcher at security firm BeyondTrust, based on the format of the “bot_ID” field assigned to each infected host, the server was collecting data from users infected with version 1.7.2 of the RaccoonStealer malware.

“Racoon is fairly typical Malware-as-a-Service where for $75-$200 per month you get access to the toolkit to generate malware payloads and a backend website to administer your campaign from,” Maude told *The Record* in an email interview last month.

“It is designed to steal login credentials, credit card information, cryptocurrency wallets, and browser information. People often don’t realize, but things like the password store on Chrome are encrypted using the Windows API. This means that if the malware is running in the user context, it can decrypt all the logins saved in the Chrome DB and steal them,” Maude said.

And according to data seen by this reporter, Maude was right. The Elasticsearch server did not only hold personal victim data like emails, usernames, and device details but was also storing cleartext passwords and even authentication cookies.

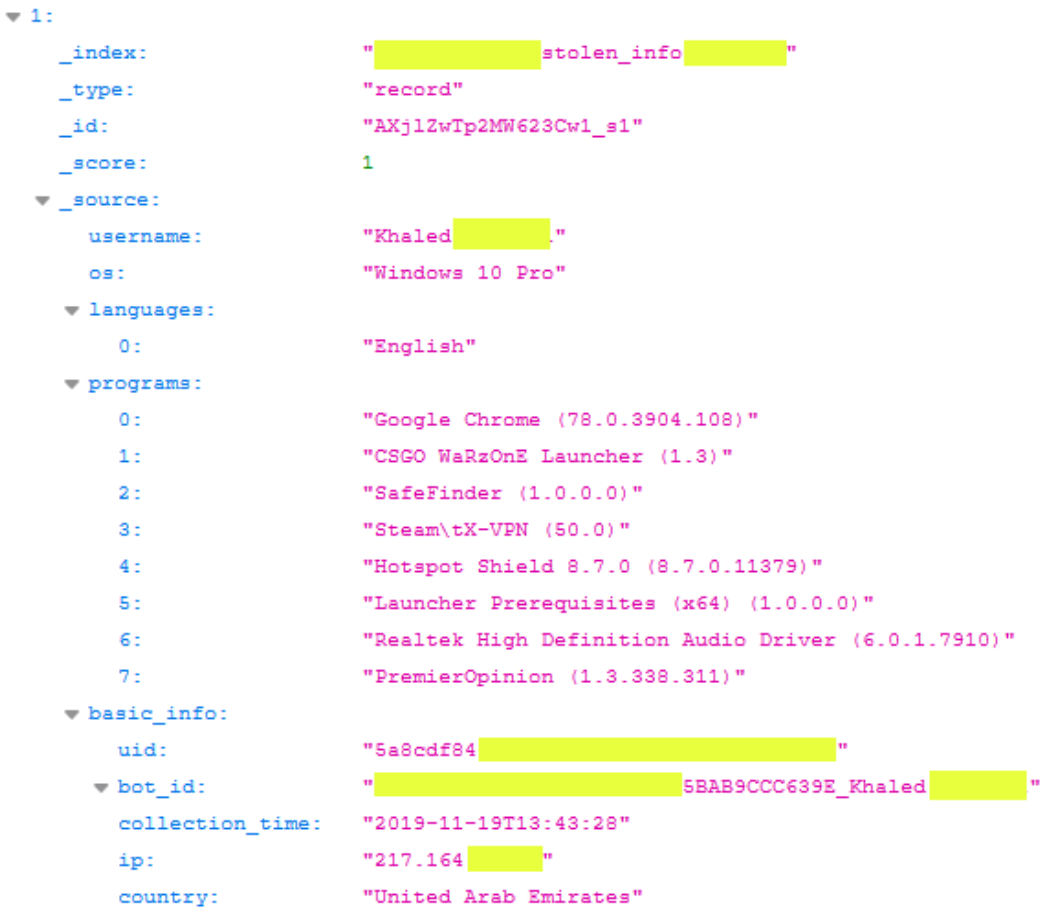

Image: The Record

Image: The Record

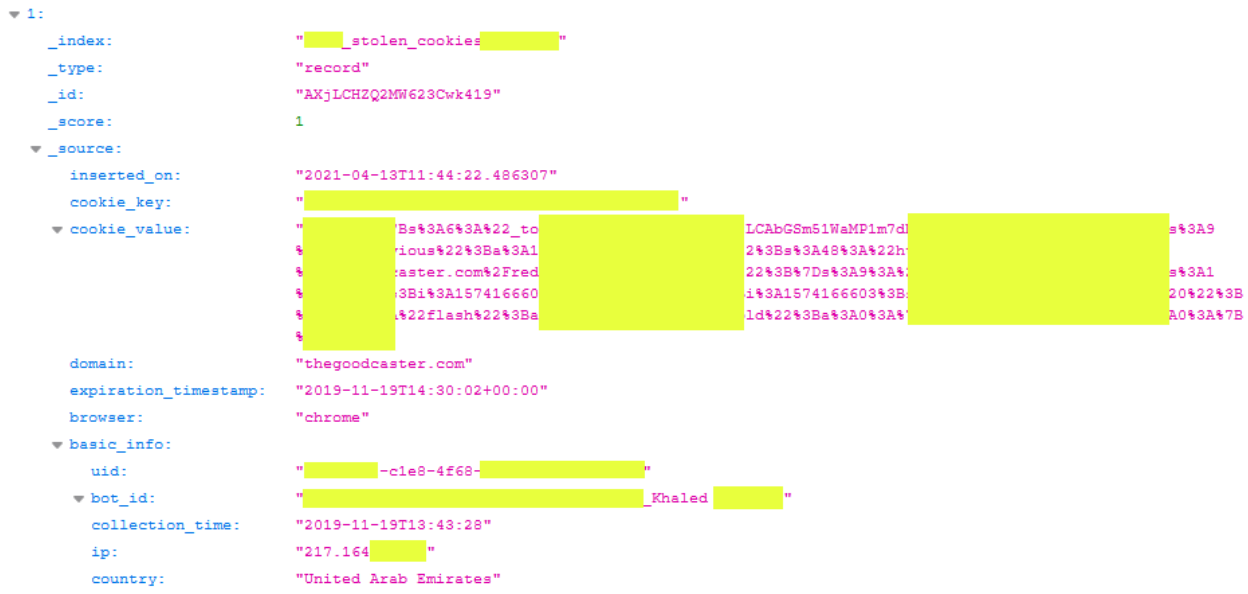

Image: The Record

In the leaked data, we found credentials and cookies for email accounts, social media profiles, work applications, and even government portals.

Of the entire data collected in the server, the most prevalent were authentication cookies, collected in the millions, rather than passwords, which were only hundreds of thousands.

The reason why the threat actor focused on stealing authentication cookies is that they allow better and easier access to an account compared to usernames and passwords.

Auth cookies, as they are also called, allow intruders to access victim accounts without needing to authenticate using usernames and passwords and even bypass any two-step verification process that victims might have had in place.

For this reason, authentication cookies are highly prized in the cybercrime ecosystem. Cybercrime marketplaces such as Genesis or RichLogs often list authentication cookies for sale on their portals.

Server disappeared today without a trace

But while Diachenko has been fighting for weeks with little success to get the cloud provider to intervene and take down this malware gang's data, the server mysteriously disappeared earlier today.

At the time of writing, it is unclear if the cloud provider finally decided to act or if the malware gang saw Diachenko and this reporter sift through the data while preparing this article.

Diachenko told *The Record* he plans to provide parts of the stolen data he discovered in the now-defunct Elasticsearch server to Troy Hunt, the operator of the Have I Been Pwned portal, so the data can be indexed and allow users to check if their account passwords and cookies were compromised. Diachenko said most of the data was for users living in the United Arab Emirates and other Middle East countries.

We will update this article when the stolen data is going to be added to HIBP, so readers can know they can check it there.

Tags

- authentication cookies
- cookies
- credentials
- data leak
- Elasticsearch
- infostealer
- leak
- malware
- passwords
- Raccoon
- RaccoonStealer

Catalin Cimpanu is a cybersecurity reporter for The Record. He previously worked at ZDNet and Bleeping Computer, where he became a well-known name in the industry for his constant scoops on new vulnerabilities, cyberattacks, and law enforcement actions against hackers.