**Specjaliści firmy Check Point wykryli w Dark Webie narzędzie online – Gazorp - służące do budowy zindywidualizowanych kopii złośliwego oprogramowania Azorult**

**Badacze bezpieczeństwa firmy Check Point, w składzie Nikita Fokin, Israel Gubi, Mark Lechtik, odkryli w sieci Dark Web narzędzie online nazywane Gazorp, które pozwala na łatwe tworzenie zindywidualizowanych plików wykonywalnych dla Azorult, złośliwego oprogramowania kradnącego dane. Kongifurator Gazorp pozwala na darmowe generowanie złośliwego kodu w celu kradzieży m.in. haseł, danych płatności czy portfelów z kryptowalutami.**

17 września badacze Check Point wykryli nowy konfigurator online, nazwany ‘Gazorp’, umieszczony w Dark Webie. Gazorp został zaprojektowany, aby budować pliki wykonywalne popularnego złośliwego oprogramowania, Azorult, programu kradnącego informacje prywatne, hasła i numery kart kredytowych.

Co więcej, usługa Gazorp jest dostępna bezpłatnie i pozwala na tworzenie świeżych próbek oprogramowania Azorult i odpowiadającego serwerowego kodu panelu sterowania, więc wystarczy tylko podać własny adres serwera C&C (Command & Control). Ten adres jest umieszczany w nowoutworzonym pliku wykonywalnym, który może być następnie rozprowadzony w dowolny sposób. Badacze Check Point dokładnie przetestowali platformę i odkryli, że Gazorp rzeczywiście tworzy kopie oprogramowania Azorult w wersji 3.0.(eksperci Check Pointa wypróbowali konfigurator Gazorp i wygenerowali działające kopie oprogramowania Azorult w wersji 3.0). Ta wersja złośliwego oprogramowania została wykryta 5 miesięcy temu i została od tego czasu zaktualizowana dwukrotnie: w atakach zostały zaobserwowane wersje 3.1 i 3.2.

Azorult występuje od co najmniej 2016 roku, badacze złośliwego oprogramowania z firmy Proofpoint [wykryli](https://securityaffairs.co/wordpress/74930/cyber-crime/azorult-fresh-campaign.html) nową wersję AZORult podczas dużego ataku emailowego 18 czerwca, jedynie 24 godziny po tym jak pojawił się na przestępczych forach w [Dark Webie](https://securityaffairs.co/wordpress/40933/cyber-crime/dark-web-cybercrime.html). Eksperci zauważyli także, że pojawienie się Gazorp w Dark Webie było skutkiem wycieku kodu panelu sterowania Azorult (dla wersji 3.1 i 3.2).

Dostępność kodu pozwala każdemu z łatwością stworzyć własną wersję panelu kontrolnego C&C Azorult, eksperci zaznaczyli również, że wyciek zawierał konfigurator najnowszej wersji złośliwego oprogramowania. Konfigurator ten nie jest oryginalnym, używanym przez autorów, „jedynie koduje i umieszcza adres C&C podany przez użytkownika i zapisuje go w pliku wykonywalnym”.

„Możliwe, że prostota tego mechanizmu i sposób dostarczania nowych wersji zainspirowała twórców Gazorpa do udostępnienia go publicznie” czytamy dalej w analizie badaczy.

Konfigurator przekierowuje do kanału Telegram używanego przez autorów do informowania użytkowników o nowościach w projekcie. Autorzy Gazorpa planują rozszerzenie istniejących funkcji dzięki modułom oraz możliwości konfigurowania panelu i eksportowania różnych baz danych do pliku.

Eksperci uważają, że możemy się niedługo spodziewać nagłego przyrostu ataków korzystających z aplikacji Azorult wygenerowanych za pomocą konfiguratora.

„Wygląda na to, że mamy do czynienia z bardzo wczesną wersją usługi Gazorp (0.1.), a głównym dostarczanym produktem jest ulepszony panel sterowania C&C Azorult. Możemy się jednak spodziewać, że projekt będzie ewoluował i powstaną nowe warianty Azorult” - podsumowują badacze Check Point.

Biorąc pod uwagę, że serwis jest darmowy, możemy się spodziewać zwiększenia ilości ataków z wykorzystaniem plików binarnych wygenerowanych przez Gazorp. Check Point zapowiedział, że będzie monitorować to zagrożenie i informować o nowościach na naszym blogu.