What's Dead May Never Die: AZORult Infostealer Decommissioned Again

ke-la.com/whats-dead-may-never-die-azorult-infostealer-decommissioned-again/

February 26, 2020

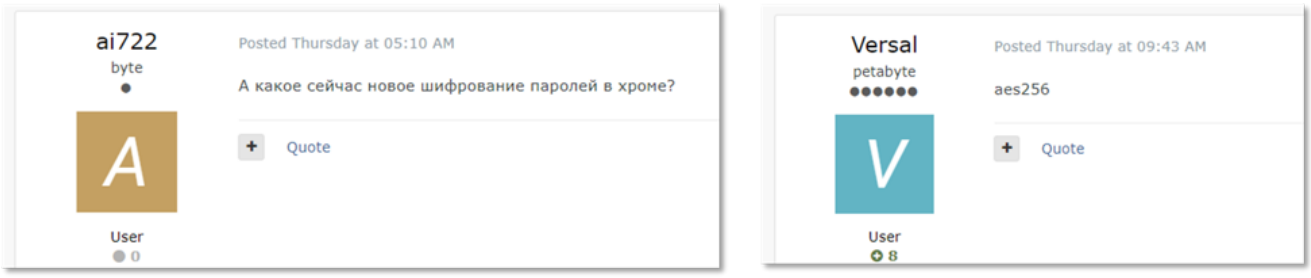
Bottom Line Up Front

Since mid-February, discussions throughout multiple cybercrime communities have been noting that the main password stealing features of the AZORult infostealer – one of the most prevalent stealers currently in use, and the main culprit behind the ongoing campaign – have been disabled by a recent Google Chrome update. Since AZORult isn't actively maintained, many actors are now regarding the stealer as fully decommissioned.

One Chrome Update to Rule Them All

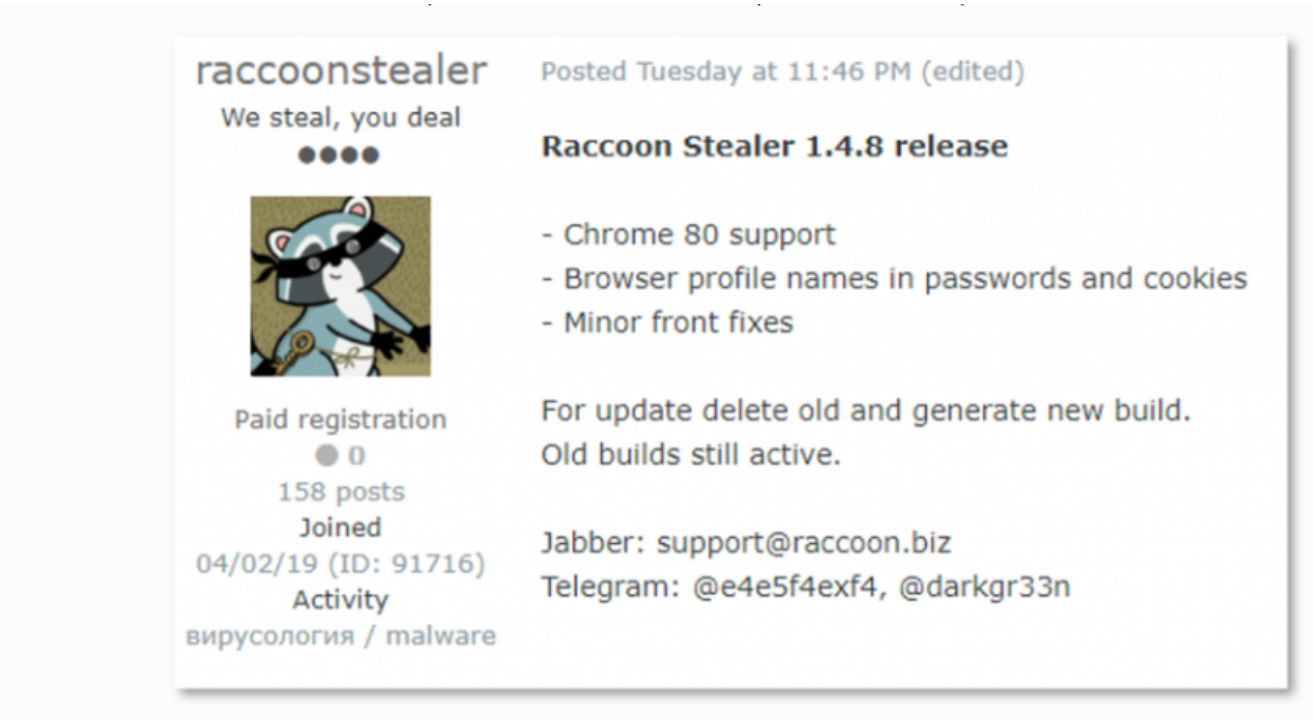
Over the last several days, threat actors in a variety of cybercrime forums have been spreading obituaries for AZORult – one of the major, most prevalent infostealers in use by the cybercrime underground. This is not the first time AZORult dies. In late 2018, sales by the official developer have stopped because the source code became too ubiquitous and sprang too many offshoots. However, as shown in our latest research, AZORult remained very active – it's been seen in recent campaigns and is directly related to over 300,000 infections paddled on the Genesis Store botnet market.

This time, the situation is different – the word around the cybercriminal underground is that AZORult is not capable of handling features bundled by a recent Google Chrome update. One of AZORult's main functions is stealing browser-saved credentials, and threat actors are claiming that Chrome's move to hashing locally-saved password in the AES-256 algorithm thwarts AZORult's best efforts to steal them.



*Top: an obituary to AZORult posted in a closed Russian hacking forum; from Russian: "Azor is finished. Not only that – **all the older cracked versions of different stealers are finished**". Bottom: actors discussing AZORult's apparent demise on a different forum. From Russian: "What is the new encryption of passwords in chrome?"; "aes256"*

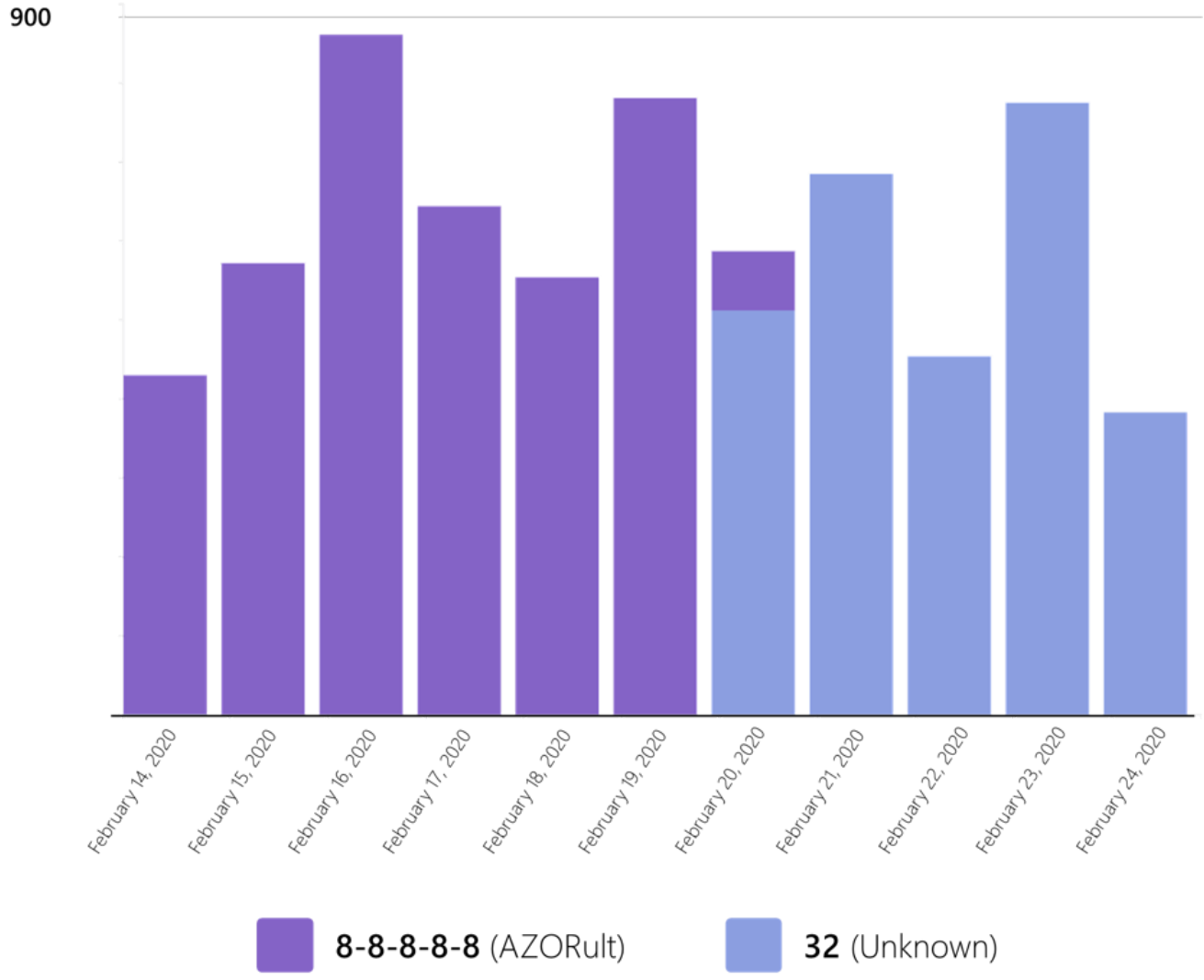
As can be seen in the excerpt above – noting "all the older cracked versions of different stealers are finished" – AZORult is not the only stealer that was affected by the update. The Raccoon stealer, for example, was also affected by the update. However, unlike AZORult, Raccoon is actively maintained by a centralized management – and as such was able to adapt the malware to bypass Chrome's effort to hide important user data. Other users have noted KPot stealer has also updated its mechanisms to cope with the new update.



Raccoon's announcement on updating the stealer to support the new Chrome release

What's Next?

AZORult's apparent demise – for now, at least – can also be tracked in Genesis. Following the methodology outlined in our latest research, we're able to notice a turning point in the last week: for the first time in over a year, Genesis ditched AZORult and went all-in on a currently-unidentified trojan as the major infection type. This showcases an important business principle: never have a single point of failure**.** The fact that Genesis was cultivating relationships with several malware providers just might have saved their business, as they were quickly able to fully pivot to a new malware.



New infections in Genesis in the past week, broken down by infection type – AZORult vs. a currently-unknown malware

---

AZORult's decommissioning in late 2018 was meant to leave a vacuum in the cybercrime financial ecosystem; many new infostealers were publishing themselves as the new replacement for seemingly-dead malware. Now, with no apparent heir to fix the deep issues caused by the new Chrome update, it seems that actors – if we're extrapolating from Genesis – have actually decided to move on to new stealers. That is, of course, unless an

actor picks up the AZORult source code and decides to adapt it to the new Chrome policies independently; a similar approach was taken by actors not long ago, when a new version of the stealer, coded in C++ opposed to its native Delphi, was found in active campaigns.

One interesting note to track would be AZORult's non-infostealing features, which might not be affected by the Chrome update – for example, it's loader modules allowing spreading of other malware following an AZORult infection – shouldn't be thwarted by the change in Chrome password encryption.

Following our detailed methodologies and targeted Dark Net research, KELA plans to keep tabs on these changes in order to effectively defend our clients from commodity malware threats.