Threatening Redirect Web Service Instills Malicious Campaigns In Over 16,500 Websites

digitalinformationworld.com/2022/04/threatening-redirect-web-service.html

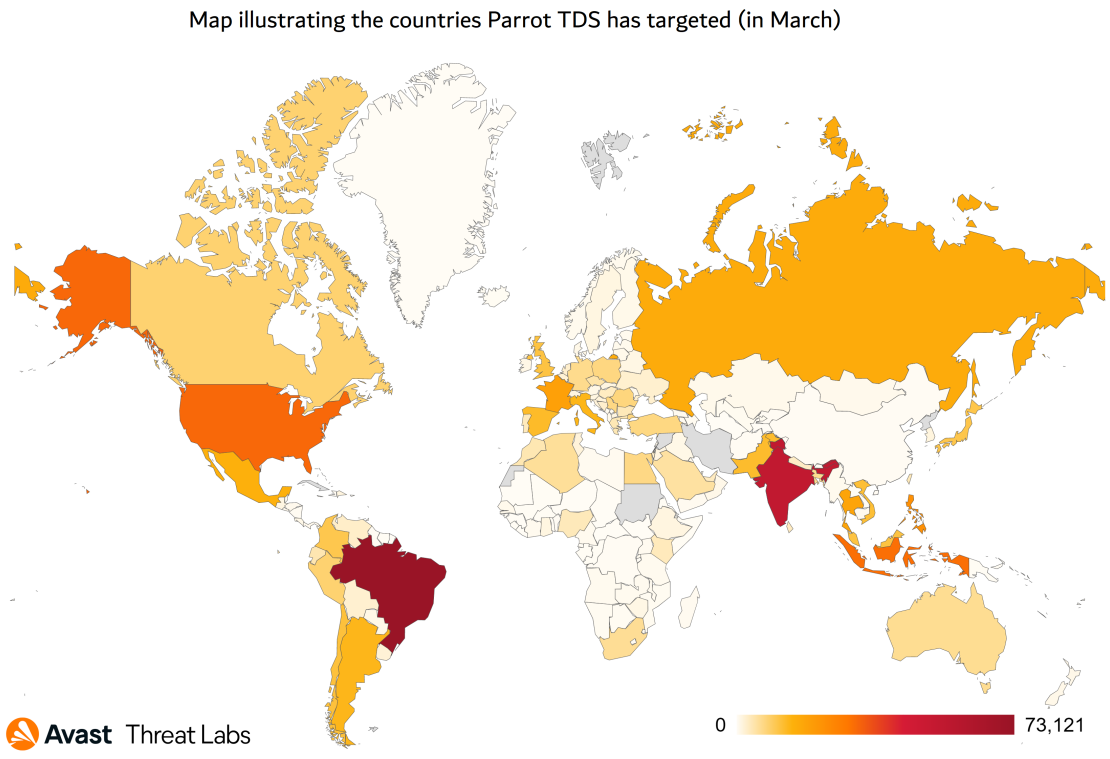
April 10, 2022

Security researchers are raising the alarm about a threatening traffic direction system named Parrot.

The new redirect service is being outlined as the root cause of infecting more than 16,500 different servers playing host to various sectors like universities, blogs, adult sites, and even local governments.

This new TDS has been known to redirect vulnerable victims that match a particular target profile towards different sources on the web like malicious sites or phishing programs.

The actors running these malicious campaigns begin the process by purchasing the TDS so they can selectively control the target that's coming in while forwarding it to another location that has a similarly malicious theme.



On a routine basis, most TDS services are used by so those who belong to the marketing sector and that's why there are credible reports showing how similar campaigns were run in the recent past too.

Parrot has been reported as being detected by security analysts that are working for Avast. They have recently made claims about how the campaign was used for FakeUpdate which used fake browsers to deliver update notices about remote access trojans, better known as RATs.

While the malicious incident may have been reported in February of this year, there are plenty of signs that show that it was very active since October of 2021.

The security analysts also shed light on how users can distinguish the alarming Parrot TDS from a number of others by how its far outreach and the number of target victims affected.

In addition, the analysts claim these malicious websites actually may not have too many similar findings other than the fact that servers hosted some unsecured CMS websites.

The new malicious web in place is based on poor servers that were laid down by hackers who directed it to a number of locations through the parroting pattern.

Last month alone, Avast was able to secure nearly 600,000 vulnerable targets through its diverse services, disabling them from paying these infected areas a visit. And that just goes to show the huge potential of the Parrot gateway.

Common nations affected by Parrot included the likes of India, Singapore, Brazil, Indonesia, and the US too. But new emerging details showed how Parrot can finetune its filters to target a particular user's profile from hundreds of others.

They are known to achieve just that by forwarding the target to special URLs that have detailed network profiles and intricately designed software.

And while the RAT initiative may be the main target for the TDS, security experts believe some of the affected servers actually serve as hosts for different phishing sites. And while their homepages may appear authentic like Microsoft's classic log-in, they are not. Therefore, users end up adding their credentials for accounts and become targeted.

But is there a solution to this problem? Well, Avast has been generous enough to outline a few pointers worth a mention:

1. Admins can scan their files using anti-virus software
2. They should replace any JavaScript files with their originals
3. Make use of the newest CMS version with extra plugins
4. Keep an eye out for tasks that run automatically
5. Make use of strong credentials for all accounts, including the use of 2FA where necessary
6. Add any security plugins for vulnerable sites like WordPress

Read next: A new malware FFDroider is hacking social media accounts by stealing browser data