PROMETHEUS|PROMETHEUS-TDS-AD|PROMETHEUS-TDS-MODUS-OPERANDI

Catalin Cimpanu

August 5th, 2021

Malware | News | Cybercrime

Meet Prometheus, the secret TDS behind some of today's malware campaigns

A recently discovered cybercrime service is helping malware gangs distribute their malicious payloads to unsuspecting users using hacked websites.

Named **Prometheus**, the service is what security researchers call a "*traffic distribution system*," also known as a TDS.

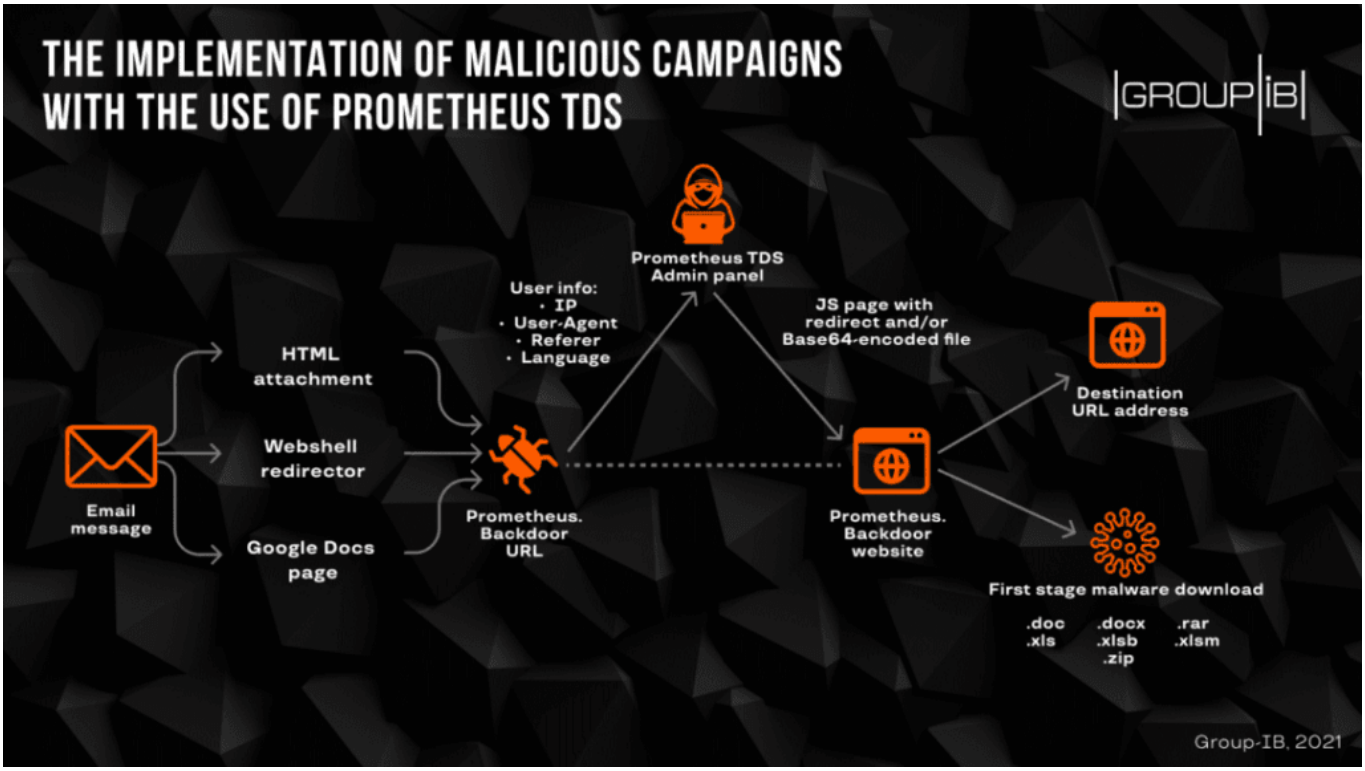
How the Prometheus TDS works

The idea is that malware gangs can rent access to Prometheus and receive an account on the TDS platform.

Buyers can then access the account, configure the malware payload they want to distribute, the type of users they want to target (based on details such as geographical location, browser or OS version), and provide a list of hacked web servers.

The Prometheus TDS will then scan the list of hacked websites and then zeploy its own backdoor to the hacked servers. Once this is done, Prometheus customers can then move on to send email spam campaigns where the email text contains links to the hacked websites.

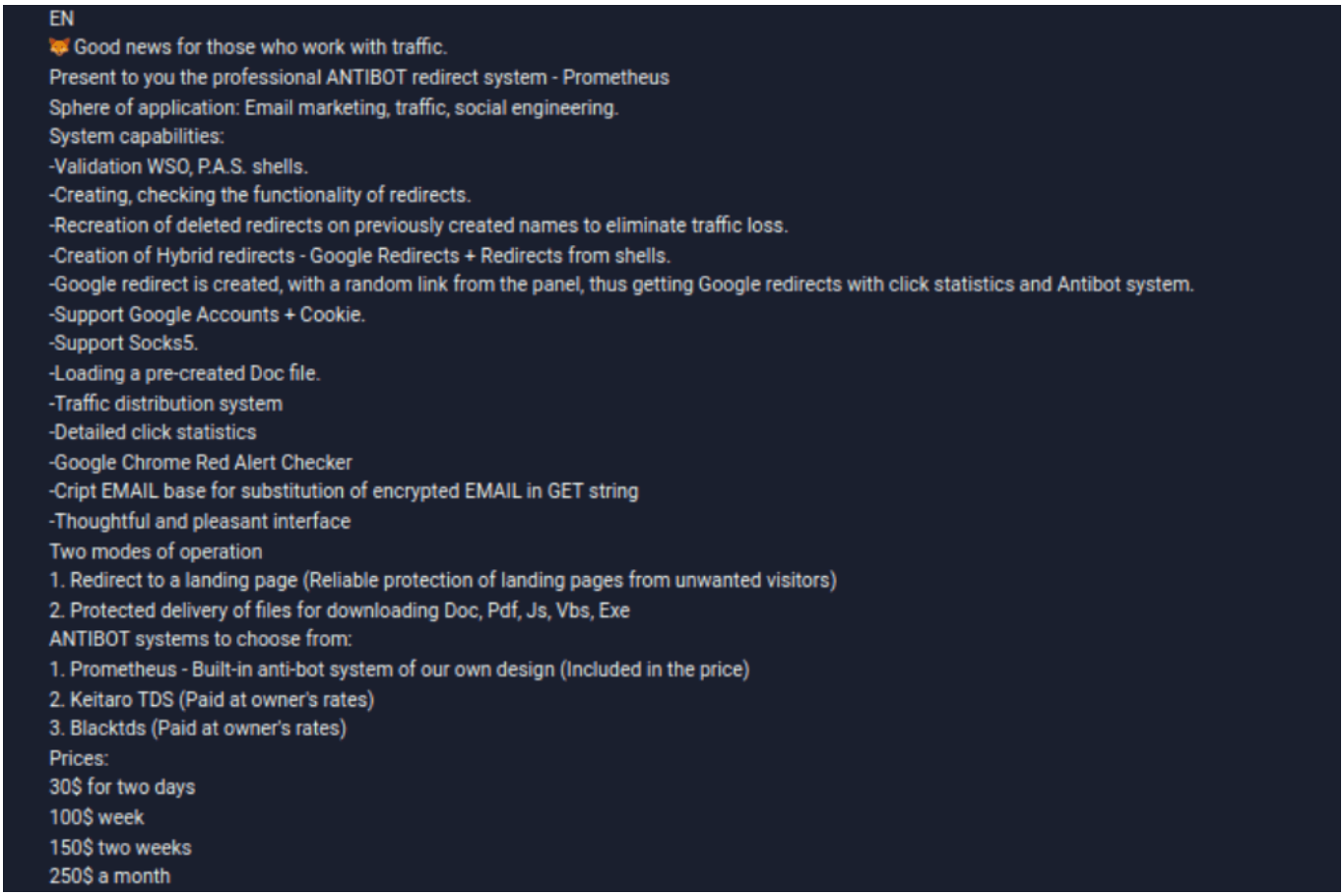
When users click the links and land on the hacked site, the Prometheus backdoor analyzes the victim's browser details and, based on the campaign parameters, will either redirect the user to a clean web page or to one that hosts a malicious file.



Spotted by security firm Group-IB earlier this spring, Prometheus is currently advertised on underground cybercrime forums for prices ranging from 30$ for 2 days of access to the platform to $250 a month.

The Prometheus ad, which dates back to August 2020, suggests the service has been live and used by malware gangs for almost a year.

Group-IB researchers said they discovered several campaigns where malware samples distributed through hacked web servers were bearing the mark and URL schemes of the Prometheus TDS, including some of today's most dangerous malware strains, such as Campo Loader, IcedID, QBot, SocGholish, and Buer Loader.



Group-IB's recent findings come to show once again that the current cybercrime ecosystem is not made up of just the people who create malware.

In almost all current malware campaigns, there are always at least two or three different groups working together to provide various services or features, which can usually include the likes of malware crypting, antivirus checkers, Office file weaponization (exploit building), spam-sending services, traffic distribution systems, and, many others.

Tags

malware US Hack Cybercrime botnet

Previous article

Next article

CATALIN CIMPANU