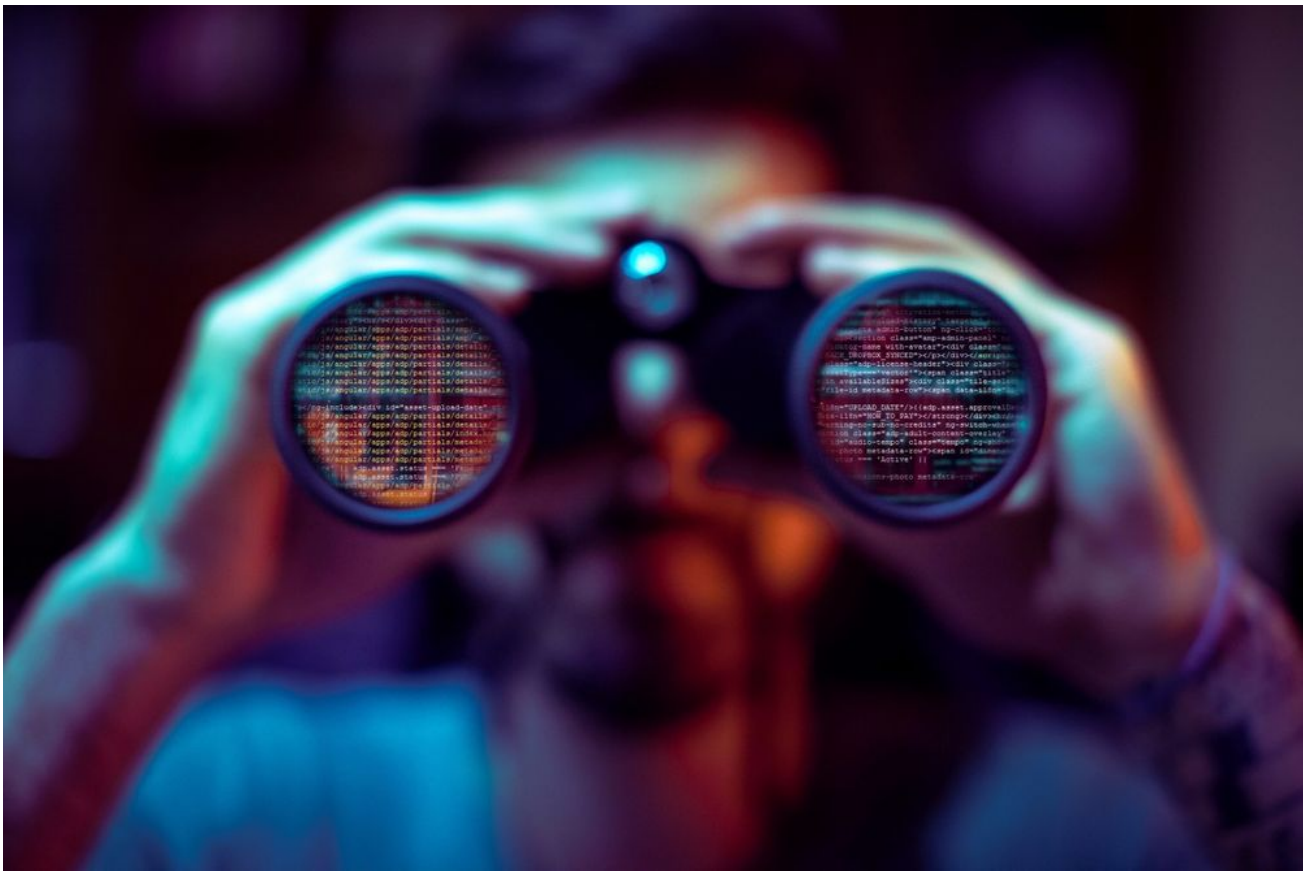
Inside Netrepser – a JavaScript-based Targeted Attack

labs.bitdefender.com/2017/05/inside-netrepser-a-javascript-based-targeted-attack/

Bogdan BOTEZATU
May 05, 2017



In May 2016, the Bitdefender threat response team isolated several samples from the internal malware zoo while looking into a custom file-packing algorithm. A deeper look into our global telemetry revealed that this piece of malware was strictly affecting a limited pool of hosts belonging to a number of IP addresses marked as sensitive targets.

Its unusual build could have easily made it pass for a regular threat like many of those that organizations block on a daily basis; however, telemetry information provided by our event correlation service has pointed out that most of its victims are government agencies. Paired with advanced spear phishing techniques and the malware's primary focus to collect intelligence and exfiltrate it systematically, we presume that this attack is part of a high-level cyber-espionage campaign.

The piece of malware we look at in this report comes with quite an array of methods to steal information, ranging from keylogging to password and cookie theft. It is built around a legitimate, yet controversial recovery toolkit provided by Nirsoft. The controversy stems from the fact that the applications provided by Nirsoft are used to recover cached passwords or monitor network traffic via powerful command-line interfaces that can be instructed to run completely covertly. For a long time now, the antimalware industry has flagged the tools provided by Nirsoft as potential threats to security specifically because they are extremely easy to abuse, and oversimplify the creation of powerful malware.

Even though the Netrepser malware uses free tools and utilities to carry various jobs to completion, the technical complexity of the attack, as well as the targets attacked, suggest that Netrepser is more than a commercial-grade tool.

Sounds interesting? Download the full whitepaper below:

Download the whitepaper

TAGS

anti-malware research whitepapers

AUTHOR

hood at @Bitdefender as director

Bookmarks