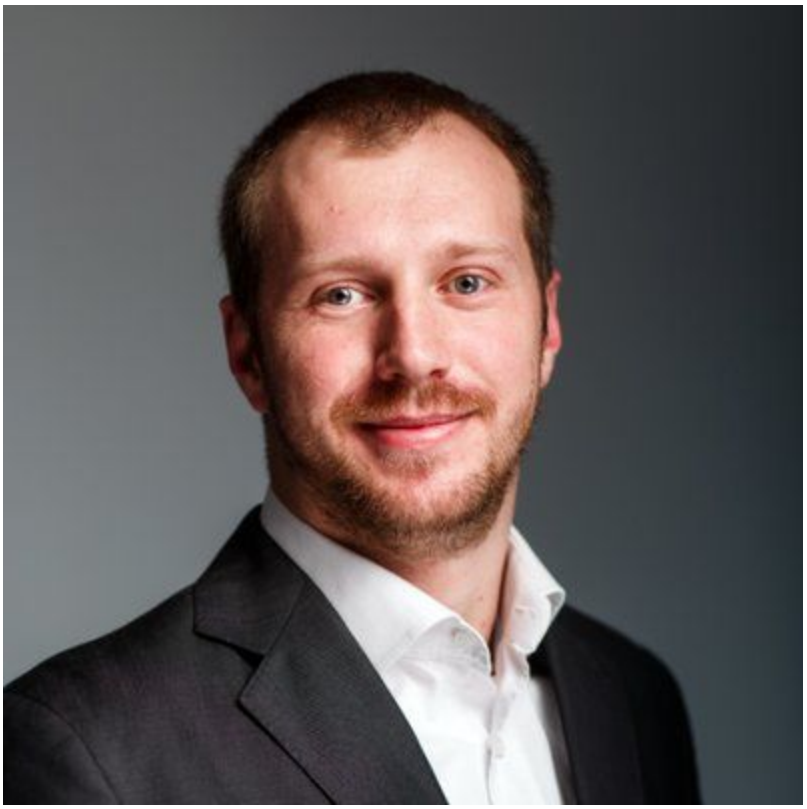
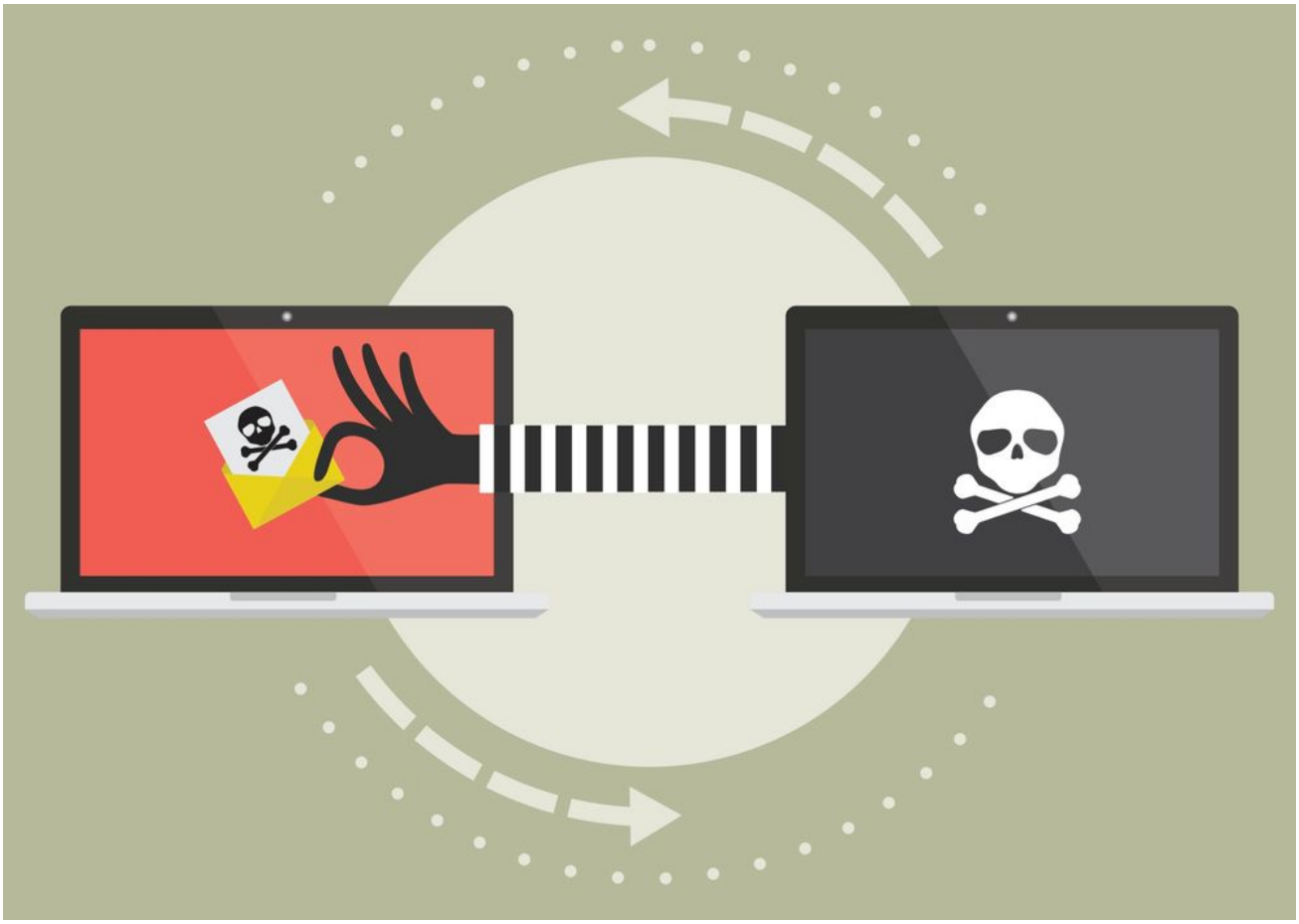
Inside Scranos – A Cross Platform, Rootkit-Enabled Spyware Operation

B labs.bitdefender.com/2019/04/inside-scranos-a-cross-platform-rootkit-enabled-spyware-operation/



Bogdan BOTEZATU
April 16, 2019



Last year, the Bitdefender Cyber Threat Intelligence Lab started analysis of a new password- and data-stealing operation based around a rootkit driver digitally signed with a possibly stolen certificate. The operation, partially described in a recent article by Tencent, primarily targeted Chinese territory until recently, when it broke out around the world.

Despite the sophistication, this attack looks like a work in progress, with many components in the early stage of development. Although the campaign has not reached the magnitude of the Zacinlo adware campaign, it is already infecting users worldwide.

We discovered that the operators of this rootkit-enabled spyware are continuously testing new components on already-infected users and regularly making minor improvement to old components. The various components can serve different purposes or take different approaches to achieving their goals. Some of the most important components shipped with the malware can achieve the following:

- Extract cookies and steal login credentials from **Google Chrome, Chromium, Mozilla Firefox, Opera, Microsoft Edge, Internet Explorer, Baidu Browser** and **Yandex Browser**.
- Steal a user's payment accounts from his **Facebook, Amazon** and **Airbnb** webpages.
- Send friend requests to other accounts, from the user's **Facebook** account.

- Send phishing messages to the victim's **Facebook** friends containing malicious APKs used to infect **Android** users as well.
- Steal login credentials for the user's account on **Steam**.
- Inject JavaScript adware in Internet Explorer.
- Install Chrome/Opera extensions to inject JavaScript adware on these browsers as well.
- Exfiltrate browsing history.
- Silently display ads or muted **YouTube**videos to users via Chrome. We found some droppers that can install Chrome if it is not already on the victim's computer.
- Subscribe users to **YouTube** video channels.
- Download and execute any payload.

Want to learn more? Download the full paper below:

Download the whitepaper

TAGS

anti-malware research whitepapers

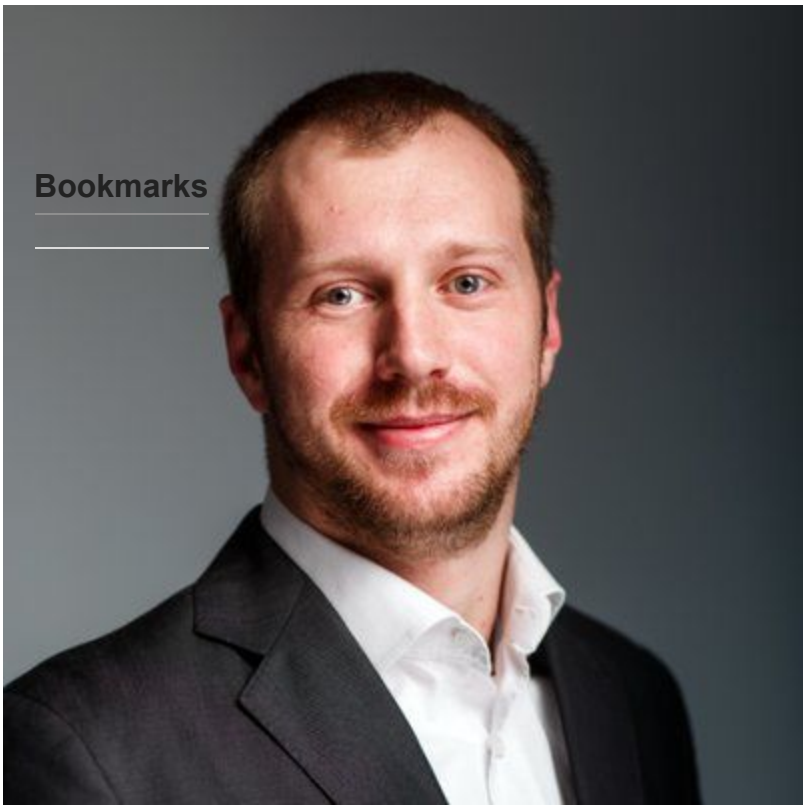
AUTHOR

Bogdan BOTEZATU

Information security professional. Living my second childhood at @Bitdefender as director of threat research.

View all posts

YOU MIGHT ALSO LIKE


Bookmarks