APT_vs_ISP.pdf

Sida 3 av 16

pag. 3

This paper exposes the contents originally designed for my participation in a conference as a speaker. This conference, originally scheduled for April 18, 2020, was later canceled (for the current year) due to the problems resulting from the COVID- 19 pandemic. For more information about it, see the link https://www.malwareanalystconference.com/.

The information contained herein relates to what I observed throughout 2019 during my analysis and research activities. For my speech I originally chose the telecommunications sector because it is a vital component for nearly every existing operating entity. Due to their critical role for today's society, these organizations are now faced with a multitude of threats in the cyber landscape ranging from targeted attacks to malicious actions attributable to the criminal or activist world. Adversaries that are targeting this sector have included those suspected by the industry of operating in support of China, Iran, Russia, Vietnam, and the Democratic People’s Republic of Korea (DPRK). Hacktivism also poses a big threat to ISP due the involvement of telco companies in government directives and digital regulations.

1. Protecting ISPs is today an high priority from a nation’s national security perspective

2. Internal research activities have shown that all the ISP-related intrusions that are attributable to organized adversaries (or APT) are aimed at digital espionage operations towards third parties or at accessing customer data / database.

Source: https://drive.google.com/file/d/1oA4YSwXLxEF-EXJcrM76Bc4_7ZfBGYE4/view