Tinker Telco Soldier Spy

troopers.de/troopers22/talks/7cv8pz/

Talk

Go back

China-based threat actors have persistently targeted the telecommunications sector for many years. In this talk, PwC Threat Intelligence (PwC TI) analysts will share their research and present on case studies for several China-based threats currently targeting telcos prolifically, including well-known threats such as GALLIUM, who PwC tracks as Red Dev 4, and lesser-known threat actors which have never been publicly disclosed before.

Specifically, Will and Ben will discuss some of the common tactics, techniques, and procedures (TTPs) these adversaries are using to compromise telcos, including some of their vulnerability preferences, and the strategic backdrop and objectives motivating this targeting.

Introduction

We'll begin by briefly setting the scene, with a discussion of the China-based threat landscape more broadly, particularly as it relates to telecommunications. This will include discussion of some of the wider targeting we've seen previously.

Red Dev 4 / GALLIUM

Next, we'll discuss a specific example: Red Dev 4 (a.k.a. GALLIUM) is a China-based threat actor which has compromised telecommunications entities globally. There has been no public reporting on GALLIUM since 2019, however, we assess that it remains active as of at least March 2022.

We will discuss some of the recent techniques we've seen Red Dev 4 use to maintain footholds within victim environments, such as the delivery of SoftEther VPN clients configured to connect to threat actor-owned infrastructure. This will allow us to demonstrate techniques to track similar activity, and to discover victims in network telemetry. We will also reference SoftEther configuration files submitted to an online multi-antivirus scanner by victims, the contained log files of which have assisted in identifying further malicious activity in victim networks.

Lastly, we will reference victimology and demonstrate how this reflects geopolitical activities and therefore suggests the targeting aligns with China's strategic aims.

Red Menshen

Next, we'll introduce a threat actor we track as Red Menshen. We first discovered this actor in 2021, when we detected a sample of a Linux backdoor we track as BPFDoor. We will briefly highlight some of the functionality of BPFDoor, and the ways in which Red Menshen uses it to maintain stealthy persistence and move laterally within victim environments.. Based on this analysis, we were able to identify victims in the telecommunications, government, and education sectors throughout Asia.

By analyzing network telemetry related to the victims we discovered, we were able to discover recent Red Menshen infrastructure, and to uncover the threat actor's upstream infrastructure. This led to the discovery of the suspected compromise of several hundred routers in Taiwan, which are used as proxies in order to access threat actor infrastructure and browse to websites.

Conclusions

We will conclude by discussing the wider motivations of China's ongoing exploitation of telecommunications providers. This spans a wide range, from targeting information on specific subscribers, to potentially developing access to core networks which can later be exploited for intelligence value. We assess that it is highly likely that telecommunications organisations will remain a key target for China-based threat actors. ***** ##### Attendee takeaways 1. The talk will advance public knowledge of nation-state cyber threats against the telecommunications industry worldwide.

1. We will share in-depth threat intelligence about sophisticated nation state threat actors that has not been publicly disclosed before, including their techniques and targeting.

2. Attendees will leave with a better understanding of how to identify, and defend against, these threat actors' operations and how to better secure their environments against compromise.

About the Speakers

Ben Jackson

Ben is a Senior Threat Intelligence Analyst and Reverse Engineer in PwC's Global Threat Intelligence team. Ben's day to day spans reverse engineering of custom and persistent malware implants, as well as analysis of upstream communications and threat actors' C2 management. He conducts technical research into threat actors with a variety of origins and motivations, with particular focus on sophisticated, espionage-motivated threats based in Russia and China.

Will Bonner

Will leads the APAC Research Team within PwC's Global Threat Intelligence team. He has 5 years experience working in the Threat Intelligence industry in the public sector, and brings expertise in analysing malware and network communications, particularly malware beaconing and victim identification. While Will has experience researching a broad range of threat actors based in various parts of the world, he currently focuses on those attributed to the APAC region.