'Stayin' Alive' Campaign in Asia - Check Point Blog

By etal

Published: 2023-10-09 · Archived: 2026-04-11 02:16:49 UTC

Highlights:

- ***Check Point Research has been tracking "Stayin' Alive", an ongoing espionage campaign operating in Asia, and primarily targeting the Telecom industry, as well as government organizations.***
- ***The "Stayin' Alive" campaign used against high-profile Asian organizations, initially targeted organizations in Vietnam, Uzbekistan, and Kazakhstan. As we conducted our analysis, we realized that it is part of a much wider campaign targeting the region.***
- ***Tools observed in the campaign are linked to 'ToddyCat'- a Chinese affiliated actor operating in the region***
- ***Check Point customers using Check Point Harmony Endpoint and Threat Emulation remain protected against the campaign detailed in this report***

In recent months, Check Point Research have diligently monitored an ongoing cyber campaign dubbed "Stayin' Alive." This relentless campaign, which has been active since at least 2021, has primarily set its sights on the Asian telecommunications industry and government organizations. As we delve into the intricacies of this campaign, we uncover a web of activities that shed light on its tactics, targets, and potential origins.

Campaign Overview

The "Stayin' Alive" campaign revolves around the deployment of downloaders and loaders, often utilized as initial infection vectors against high-profile Asian entities. The campaign's initial discovery, a downloader called CurKeep, zeroed in on countries like Vietnam, Uzbekistan, and Kazakhstan. However, our ongoing analysis has unveiled a much broader operation encompassing the entire region.

What makes this campaign particularly intriguing is the simplistic nature of the tools involved. They exhibit a wide variation and appear to be disposable, primarily serving as conduits for downloading and executing additional malicious payloads. These tools do not share code similarities with any known cyber actor's products and exhibit little resemblance to each other. Yet, they all trace back to a common infrastructure, linked to ToddyCat, a threat actor with Chinese affiliations operating within the region.

Key Highlights

1. Targets and Geography: "Stayin' Alive" primarily targets the telecommunications industry across Asia, with a focus on countries such as Kazakhstan, Uzbekistan, Pakistan, and Vietnam.

2. Infection Tactics: The campaign employs spear-phishing emails to deliver archive files using DLL side-loading techniques. Notably, it exploits a vulnerability in Audinate's Dante Discovery software (CVE-2022-23748) by hijacking dal_keepalives.dll.

3. Loader Diversity: Threat actors behind the campaign leverage multiple unique loaders and downloaders, all linked to the same infrastructure.

4. Basic Yet Variable Functionality: Backdoors and loaders used in the campaign exhibit basic functionality that varies widely. This suggests they are considered disposable and are primarily used to gain initial access.

Victimology

Throughout our investigation, a consistent pattern of targeting has emerged, focusing on Asian countries such as Vietnam, Pakistan, Uzbekistan, and Kazakhstan. Evidence points to spear-phishing emails, VirusTotal submissions, and file naming conventions as indications of this campaign's primary targets within the telecom sector.

The Telecommunications sector is a lucrative target for nation state-backed espionage campaigns. According to Check Point Research, since the beginning of 2023, we have seen a global weekly average of 1,504 attacks per organization in the communication industry. In Asia, we observed an average of 1,978 attacks in the same industry, which is 32% higher.

The telecommunications sector consistently face such large numbers of attacks due to the connectivity and control these telcos have of different key infrastructures, as well as storage of sensitive information about individuals that use these telco services, which could be sold on the dark web for a huge profit.

Moreover, domains associated with various loaders and downloaders suggest that at least some of the targets, or their final targets, belong to government-affiliated organizations, predominantly in Kazakhstan. These domains include mimics of the Kazakhstan National Certificate Authority (pki.gov.kz) and certexvpn, a VPN software used by the Kazakh government.

Attribution

The "Stayin' Alive" campaign represents only a fraction of a more extensive operation involving numerous unknown tools and techniques. These custom-made tools are likely highly disposable, with no discernible code overlaps to known toolsets, including each other. However, they all share ties to infrastructure associated with ToddyCat, a threat actor previously linked to Chinese espionage activities.

While it's not definitively confirmed that ToddyCat is behind the "Stayin' Alive" campaign, there is a clear connection through shared infrastructure. Furthermore, ToddyCat has been reported operating in the same countries as the "Stayin' Alive" campaign.

Conclusions

In our report, we have provided insights into the tools and techniques used in this campaign, unraveling the connections between various backdoors through their infrastructure fingerprints. Additionally, we've highlighted a potential link to ToddyCat, a known Chinese – affiliated actor in the region. While absolute certainty about ToddyCat's involvement remains elusive, the shared infrastructure and similar targeting objectives suggest a significant connection.

Check Point customers remain protected against this campaign and the threats involved by while using Check Point Harmony Endpoint, and Threat Emulation– which provides comprehensive coverage of attack tactics, file-types, and operating systems

For a more detailed analysis, we encourage readers to explore our full report on [research.checkpoint.com] (https://research.checkpoint.com).
