Check Point Research reveals a malicious firmware implant for TP-Link routers, linked to Chinese APT group

By etal

Published: 2023-05-16 · Archived: 2026-04-15 02:05:54 UTC

Highlights

- Check Point Research (CPR) exposes a malicious firmware implant for TP-Link routers which allowed attackers to gain full control of infected devices and access compromised networks while evading detection.
- CPR attributes the attacks to a Chinese state-sponsored APT group dubbed “Camaro Dragon”. The group overlaps with activity previously attributed to Mustang Panda.
- The deployment method of the firmware images remains uncertain, as does its usage and involvement in actual intrusions.

Executive Summary

Recently, Check Point Research investigated a sequence of targeted cyberattacks against European foreign affairs entities and attributed them to a Chinese state-sponsored Advanced Persistent Threat (APT) group dubbed “Camaro Dragon” by CPR. This activity has significant infrastructure overlaps with activities publicly linked to “Mustang Panda”. Our investigation discovered a malicious firmware implant created for TP-Link routers containing various harmful components, including a customized backdoor named “Horse Shell.” This backdoor enabled attackers to take full control of the infected device, remain undetected, and access compromised networks. CPR’s thorough analysis exposed these malicious tactics and provides a deep dive analysis

This blog post will delve into the intricate details analyzing the “Horse Shell” router implant and share our insights into the implant’s functionality and compare it to other router implants associated with other Chinese state-sponsored groups. By examining this implant, we hope to shed light on the techniques and tactics utilized by the Camaro Dragon APT group to provide a better understanding of how threat actors utilize malicious firmware implants in network devices for their attacks.

The Attack

Our investigation of the ‘Camaro Dragon’ activity was of a campaign targeted mainly at European foreign affairs entities. However, even though we found Horse Shell on the attacking infrastructure, we do not know who the victims of the router implant are.

Learning from history, router implants are often installed on arbitrary devices with no particular interest, with the aim to create a chain of nodes between the main infections and real command and control. In other words,

infecting a home router does not mean that the homeowner was specifically targeted, but rather that they are only a means to a goal.

We are unsure how the attackers managed to infect the router devices with their malicious implant. It is likely that they gained access to these devices by either scanning them for known vulnerabilities or targeting devices that used default or weak and easily guessable passwords for authentication. Our findings not only contribute to a better understanding of the Camaro Dragon group and their toolset, but also to the broader cybersecurity community, providing crucial knowledge for understanding and defending against similar threats in the future.

Not only TP-Link

The discovery of the firmware-agnostic nature of the implanted components indicates that a wide range of devices and vendors may be at risk.

Furthermore, our discovery of the firmware-agnostic nature of the implanted components indicates that a wide range of devices and vendors may be at risk. We hope that our research will contribute to improving the security posture of organizations and individuals alike. In the meantime, remember to keep your network devices updated and secured, and beware of any suspicious activity on your network

Protecting Your Network

The discovery of Camaro Dragon's malicious implant for TP-Link routers highlights the importance of taking protective measures against similar attacks. Here are some recommendations for detection and protection:

- **Software Updates**
  Regularly updating the firmware and software of routers and other devices is crucial for preventing vulnerabilities that attackers may exploit.
- **Default Credentials**
  Change the default login credentials of any device connected to the internet to stronger passwords and use multi-factor authentication whenever possible. Attackers often scan the internet for devices that still use default or weak credentials.
- **Use Check Point Products**
  Check Point's network security solutions provide advanced threat prevention and real-time network protection against sophisticated attacks like those used by the Camaro Dragon APT group. This includes protection against exploits, malware, and other advanced threats. Check Point's **Quantum IoT Protect** automatically identifies and maps IoT devices and assesses the risk, prevents unauthorized access to and from IoT/OT devices with zero-trust profiling and segmentation, and blocks attacks against IoT devices.

Manufacturers can do better to secure their devices against malware and cyberattacks. New regulations in the US and in Europe require vendors and manufacturers to ensure that devices do not pose risks to users and to include security features inside the device.

Check Point IoT Embedded with Nano Agent® provides on-device runtime protection enabling connected devices with built-in firmware security. The Nano Agent® is a customized package which provides the top security capabilities and prevents malicious activity on routers, network devices and other IoT devices. Check Point IoT

Nano Agent® has advanced capabilities of memory protection, anomaly detection, and control flow integrity. It operates inside the device, and serves as a frontline to secure IoT devices.
