Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ACTOR REPORT

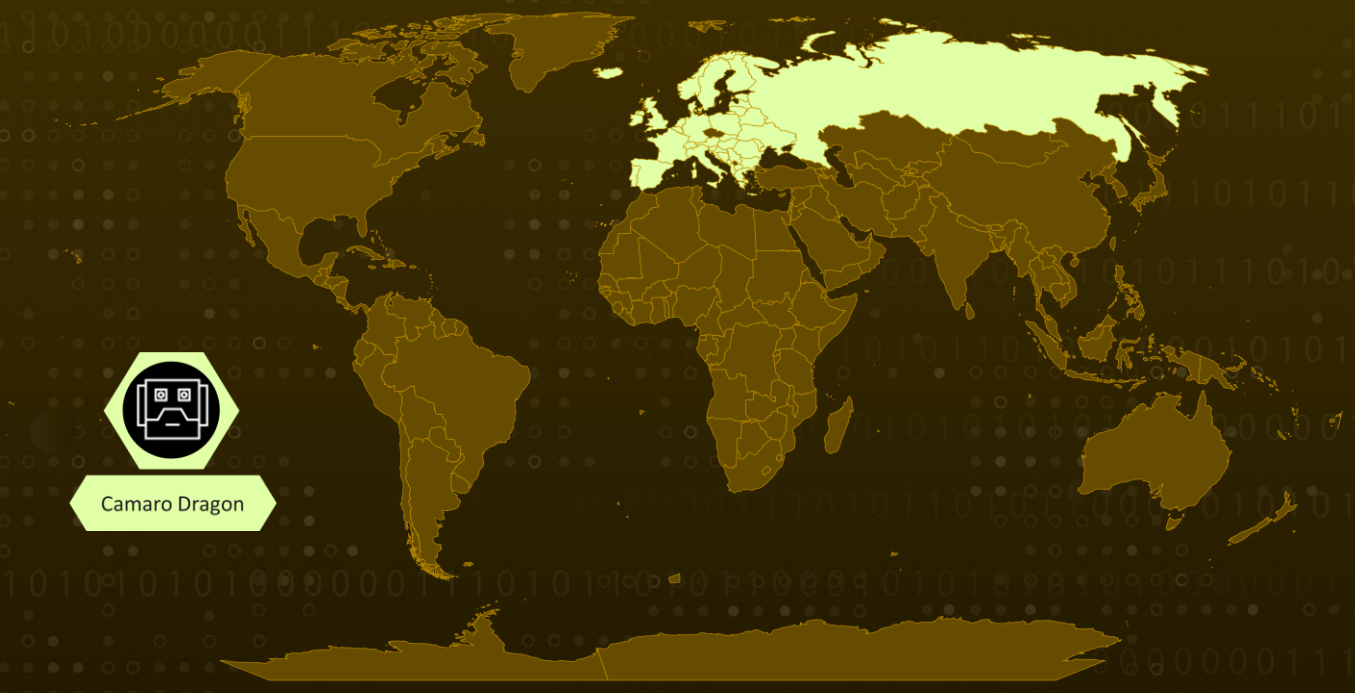
Camaro Dragon Targets European Foreign Affairs with Malicious Firmware Implant

Date of Publication	Admiralty Code	TA Number
May 19, 2023	A1	TA2023237

Summary

First Appearance: January 2023
Actor Name: Camaro Dragon
Target Region: Europe
Target Sectors: Foreign Affairs Entities

Actor Map



Actor Details

#1

Camaro Dragon is a Chinese state-sponsored advanced persistent threat (APT) group that has been targeting European foreign affairs entities. This group, believed to be linked to the Mustang Panda APT group, has been carrying out targeted attacks using a malicious firmware implant designed for TP-Link routers. The implant, named "Horse Shell," enables the attackers to maintain persistent access, establish anonymous infrastructure, and move laterally within compromised networks.

#2

The Horse Shell implant provides the attackers with three main functionalities. First, it allows for remote shell execution, enabling them to run arbitrary commands on the infected routers. Second, it enables file transfer, allowing the attackers to upload and download files to and from the compromised routers. Lastly, it supports SOCKS tunneling, which allows the relay of communication between different clients.

#3

The implant's components are firmware-agnostic, meaning they can be integrated into various firmware versions by different vendors. The exact method of deploying the firmware images onto the infected routers is still unclear, as well as its involvement in actual intrusions.

Actor Group

NAME	ORIGIN	TARGET REGIONS	TARGET INDUSTRIES
Camaro Dragon	China	Europe	foreign affairs entities
	MOTIVE		
	Information theft and espionage		

Recommendations

Update router firmware: Immediately update the firmware of TP-Link routers or any affected router models to the latest version provided by the vendor. Regular firmware updates can help patch known vulnerabilities and protect against exploits used by the Camaro Dragon group.

Implement network monitoring: Deploy network monitoring tools to keep a close watch on router activity. Look for any unusual network traffic patterns or suspicious activities that may indicate a compromised router. Timely detection can help mitigate the impact of the Camaro Dragon APT group's attacks.

Educate employees on cybersecurity: Conduct cybersecurity awareness training for employees, specifically addressing the risks associated with phishing emails, social engineering, and suspicious downloads. By educating employees about these threats, you can reduce the likelihood of successful initial compromises by the Camaro Dragon group.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0003 Persistence	TA0005 Defense Evasion	TA0008 Lateral Movement
TA0011 Command and Control	T1566 Phishing	T1189 Drive-by Compromise	T1542 Pre-OS Boot
T1542.001 System_Firmware	T1542.003 Bootkit	T1095 Non-Application Layer Protocol	T1210 Exploitation of Remote Services

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	998788472cb1502c03675a15a9f09b12f3877a5aeb687f891458a414b8e0d66c 7985f992dcc6fcce76ee2892700c8538af075bd991625156bf2482dbfebd5a5a ed3d667a4fa92d78a0a54f696f4e8ff254def8d6f3208e6fe426dbe7fb3f3dd0 66cc81a7d865941cb32ed7b1b84b20270d7d667b523cab28b856cd4e85f135b6 8a2e9f6c2b0c898090fdce021b3813313e73a256a5de39c100bf9868abc09dbb da046a1fe6f3b94e48c24ffd341f8d97bfc06252ddf4d332e8e2478262ad1964
Domains	m.cremessage[.]com
IPV4	91.245.253[.]72

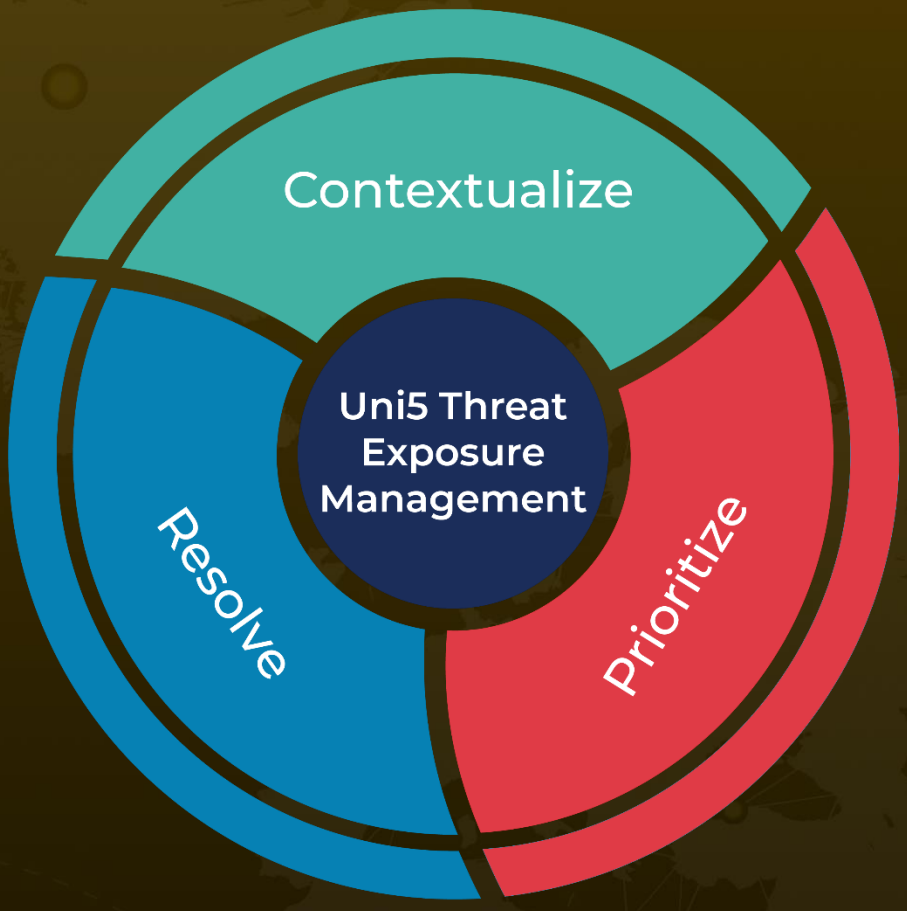
References

https://research.checkpoint.com/2023/the-dragon-who-sold-his-camaro-analyzing-custom-router-implant/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

May 19, 2023 • 5:30 AM

More at www.hivepro.com