

China-Nexus APT Targets Qatar

 blog.checkpoint.com/research/china-nexus-activity-against-qatar-observed-amid-expanding-regional-tensions

rohann@checkpoint.com

March 9, 2026



Key Findings

- Since the recent escalation in the Middle East, Check Point Research has observed increased activity by Chinese-nexus APT actors in the region, particularly targeting **Qatar**
- The Chinese-nexus threat actor **Camaro Dragon** attempted to deploy a variant of PlugX malware against Qatari targets **within one day** of the launch of Operation Epic Fury and the onset of the escalation in the Middle East
- The attackers leveraged the ongoing war in the Middle East to make their lures more credible and engaging, demonstrating the ability to rapidly adapt to major developments and breaking news
- The use of payloads such as PlugX and Cobalt Strike demonstrates a preference for simple, accessible tools that support rapid initial deployment

Missile Strikes in Bahrain as a Lure

On March 1st, one day after the start of the escalation in the Middle East, Check Point Research began observing targeted campaigns against entities in Qatar. The campaigns relied on conflict-related content as lures, intended to blend into legitimate, fast-moving regional communications.

In the first infection chain identified by Check Point Research, the threat actor delivered an archive disguised as photos of attacks on American bases in Bahrain.

الدمار الذي أصاب محيط القاعدة الأمريكية في البحرين بعد سقوط صاروخ إيراني

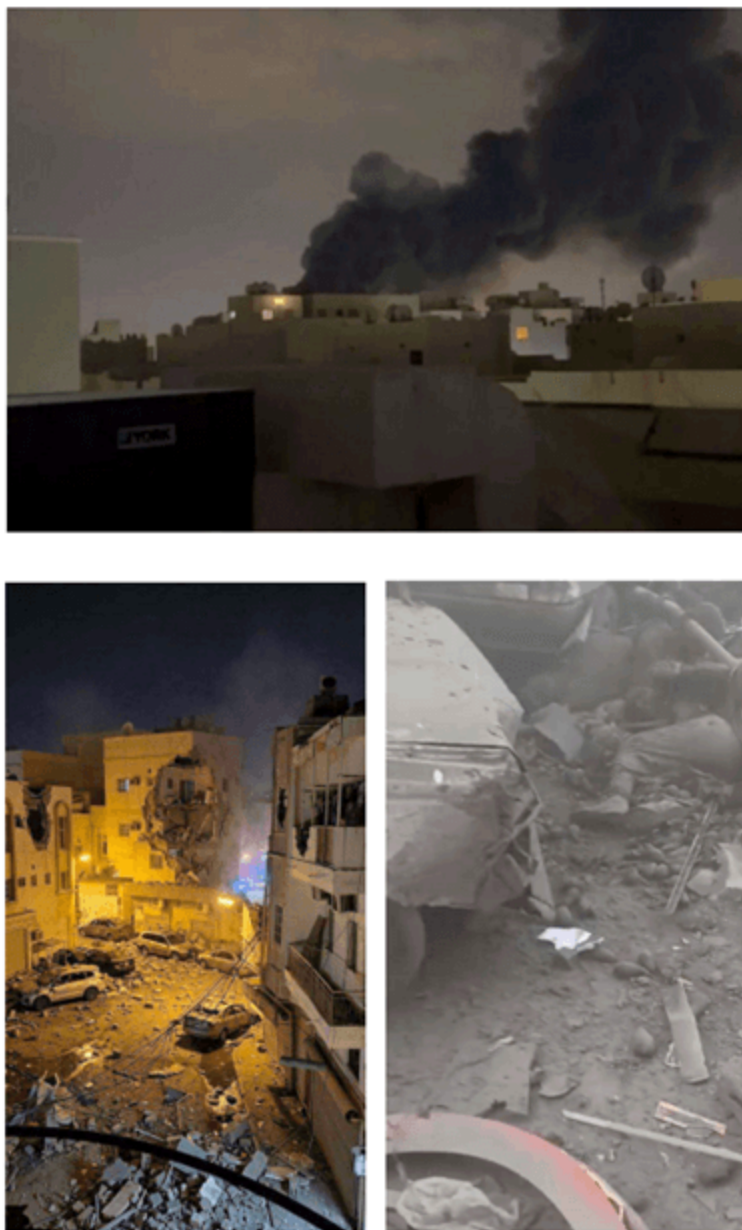


Figure 1 – Lure titled “The destruction caused by an Iranian missile strike around the US base in Bahrain”.

When executed, a LNK file from the archive starts an **unusually long infection chain**: it contacts a compromised server to retrieve the next-stage payload, eventually abusing DLL hijacking of the legitimate Baidu NetDisk binary to deploy the **PlugX backdoor**.

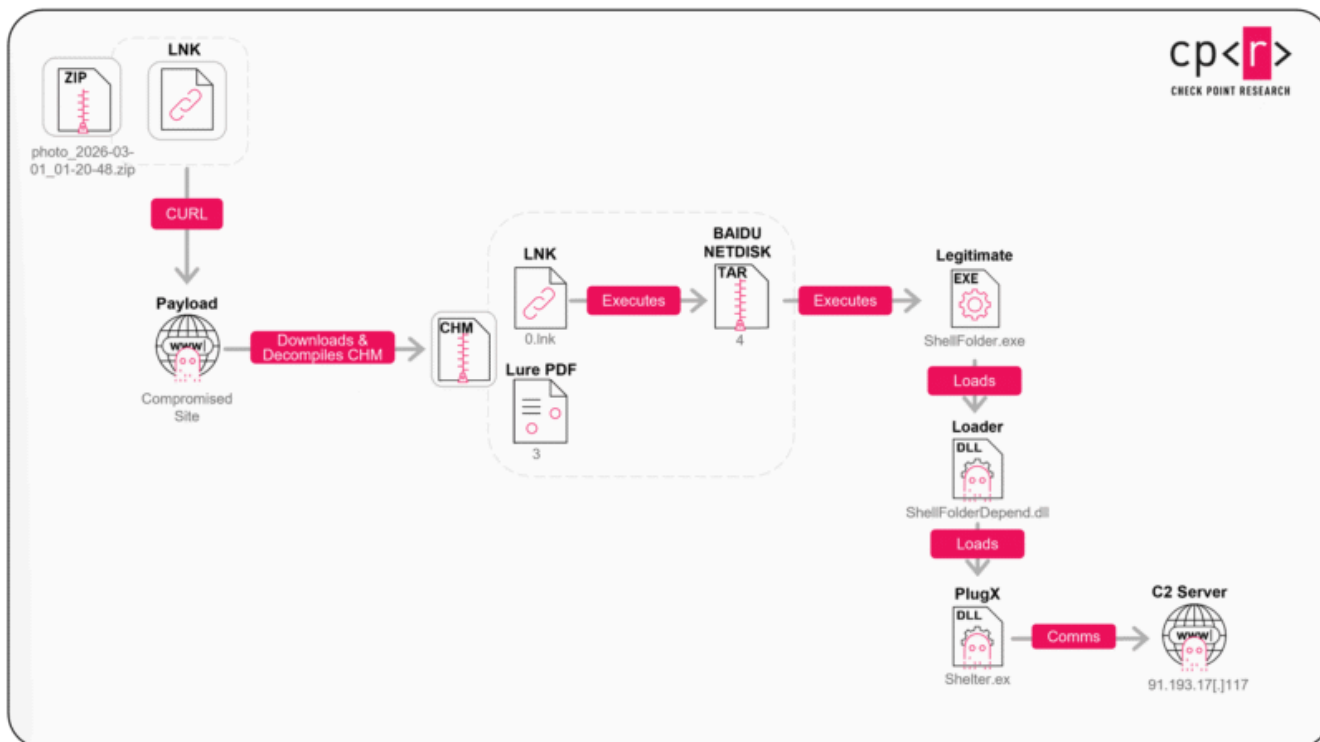


Figure 2 – Infection chain used to deploy PlugX.

PlugX is a modular backdoor associated with multiple Chinese-nexus threat actors since at least 2008. Its plugin-based architecture enables remote access and a wide range of post-compromise functions, including file exfiltration, screen capture, keystroke logging, and remote command execution.

The PlugX sample uses the configuration encryption key `qwedfgx202211` together with a date-formatted payload decryption key (`20260301@@@` in this instance), both of which have been observed in prior campaigns attributed to [Camaro Dragon](#), the China-nexus APT overlapping with clusters publicly reported as [Earth Preta](#) and Mustang Panda.

It is worth noting that this infection vector was not unique to the Qatar campaign. Check Point Research observed the same delivery method several months earlier, in late December, in attacks against Turkish military targets. This consistency suggests that the cluster maintains a broader Middle East targeting focus, with operations now shifting toward entities in Qatar as the current regional environment creates new targeting opportunities.

Strike at Gulf Oil and Gas Facilities as a Lure

In a separate campaign, Check Point Research observed another attack presumably targeting Qatar and using a password-protected archive named `Strike at Gulf oil and gas facilities.zip`, likely delivered via email. The campaign employed low-quality AI-generated lures impersonating the Israeli government to deliver a previously unseen Rust-based loader. This loader exploits DLL hijacking of `nvdaHelperRemote.dll`, a component of the open-source screen reader NVDA. Abuse

of this component has previously been observed in only a limited number of Chinese-nexus campaigns, including China-aligned activity associated with a [campaign](#) delivering **Voldemort** backdoor, as well a wave of attacks targeting the **Philippines and Myanmar** back in 2025.

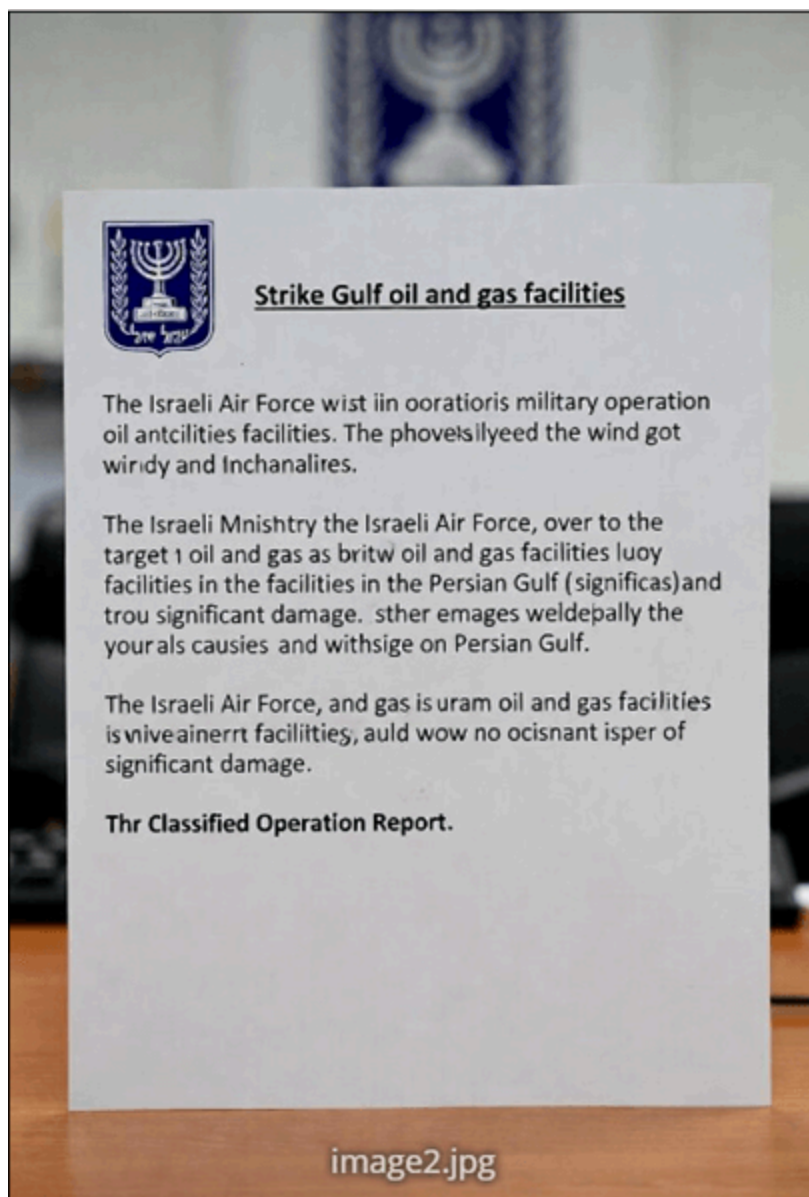


Figure 3 – Lure used as part of the Cobalt Strike infection.

The final payload deployed in this operation was **Cobalt Strike**, a well-known penetration testing framework that is often repurposed for malicious activity.

Threat actors frequently use it as an initial-stage payload to perform rapid reconnaissance on newly compromised systems and networks, allowing them to assess the environment and determine whether deeper full-on intrusion activity is justified.

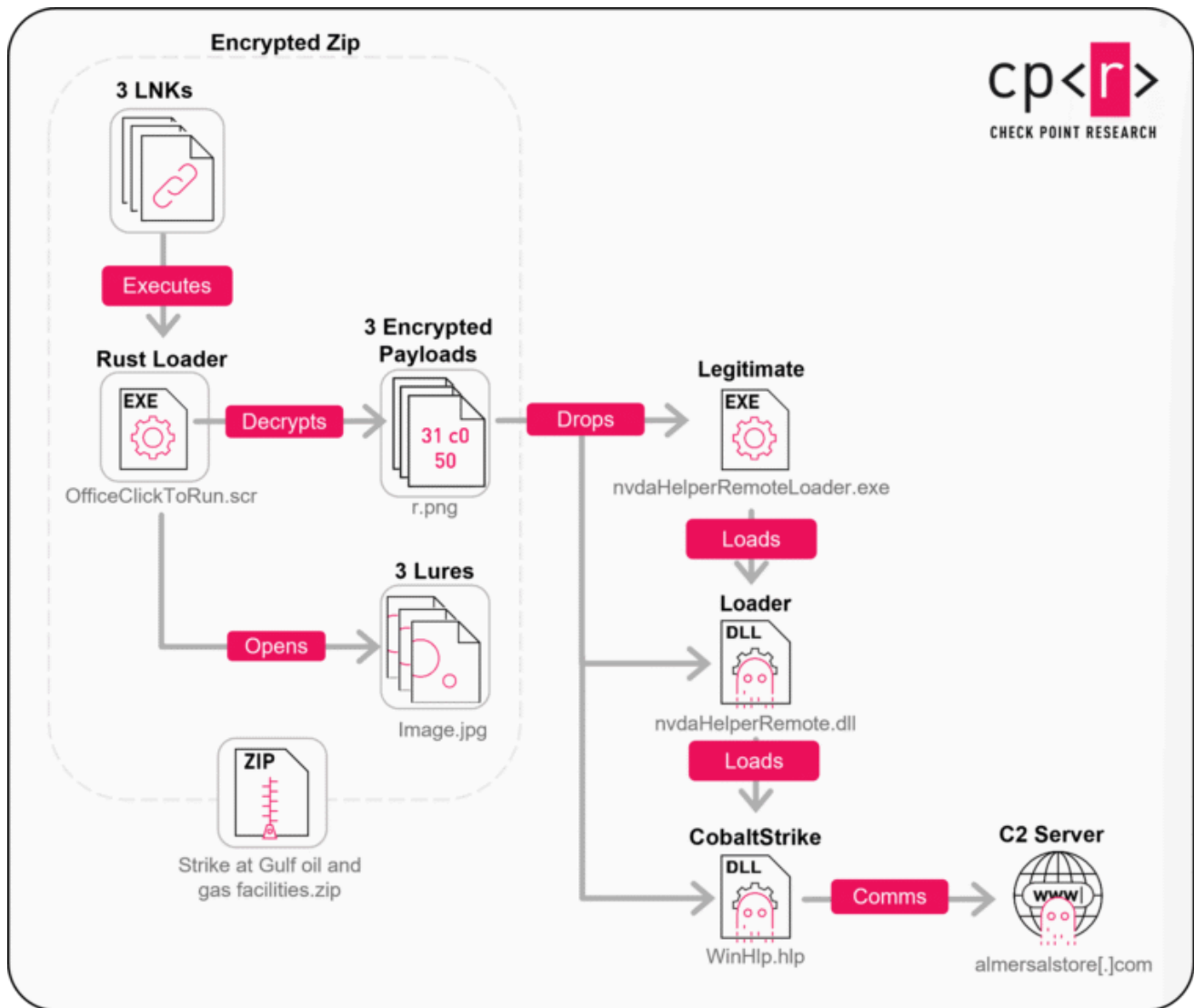


Figure 4 – Infection chain used to deploy CobaltStrike.

With low confidence, this attack is assessed as China-aligned. The use of DLL hijacking using NVDA components, Cobalt Strike, and C2 infrastructure registered via Kaopu Cloud and Cloudflare matches TTPs previously associated with Chinese threat actors, while the attack timestamps provide additional supporting context.

Outlook: Chinese Nexus Actors Shift its Focus in the Middle East

The Gulf region has not been as prominently featured in public reporting on China-nexus activity as some other parts of the broader Middle East. However, the activity observed in these campaigns suggests that major regional developments can quickly reshape priorities. In the immediate aftermath of the escalation in the Middle East, Check Point Research observed at least two separate threat actors targeting entities in Qatar using conflict-related lures tailored to blend into the region's fast-moving communications environment. Taken together, these intrusions highlight how rapidly China-nexus espionage actors can pivot in response to geopolitical events. The near-immediate focus on Qatar may reflect not only opportunistic intelligence collection tied to the regional crisis, but also a broader shift in collection priorities toward a state that sits at the intersection of several competing regional and global powers and interests.

IOCs

4d8027424b5bcd167ab70c8320ce3c5df72a9ecca01246b095e4af498f77725d
fff7864019b651bea2448228d6557d995edc929276bb9d8cb34c3c280a42684e
fa3a1153018ac1e1a35a65e445a2bad33eac582c225cf6c38d0886802481cd43
a7c56033f2264c71b0485da693e3f627b2b5ccfe3399a53cc558be77f95d9c13
c78eb1cecef5f865b6d150adcf67fa5712c5a16b94f1618c32191e61fbe69590
1ddbed0328a60bb4f725b4ef798d5d14f29c04f7ffe9a7a6940cacb557119a1c
26d10996fd2880441445539cd8a6e7fe0777f6ca3352dae6ef84d1d747aabb0c
185.219.220.73
91.193.17.117

a9de383c6a1b00c9bd5a09ef87440d72ec7fc4bcd781207b3cace2f246788d4d
b58ec14b0119182aef12d153280962ad76c30e3cd67533177d55481704eba705
a8acb9864e6f64323ed75e69038ca9bfe76f7b1b0d24ec7df8ac07b6dbd641a3
almersalstore[.]com