The Naikon APT and the MsnMM Campaigns

By Kurt Baumgartner

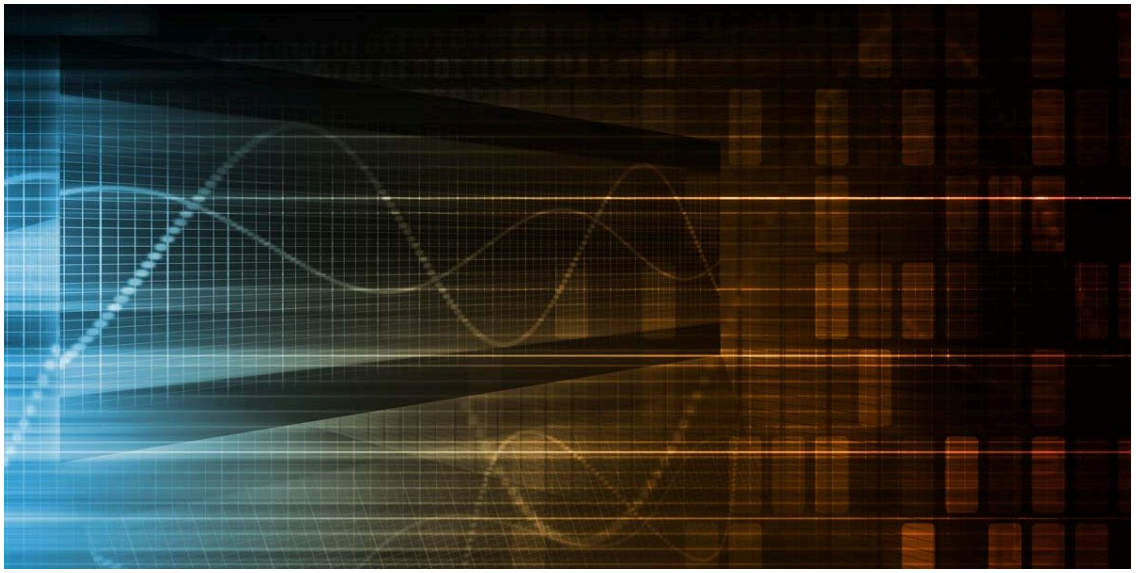
Published: 2015-05-21 · Archived: 2026-04-06 03:12:26 UTC

APT reports

APT reports

21 May 2015

2 minute read



The First Known Naikon APT Campaigns

The MsnMM Campaigns [pdf]

For over half a decade, the Naikon APT waged multiple attack campaigns on sensitive targets throughout South-eastern Asia and around the South China Sea. It maintained a heavy offensive focus on Myanmar, Vietnam, Singapore, the Philippines, Malaysia, and Laos. Targets and victims included ASEAN governmental agencies and government departments, investment enterprises, military, law enforcement and border control organizations, embassies, university faculties and others.

Parts of the campaigns have been publicly discussed according to the nature of their tools. For example, the MsnMM backdoors started out with internal names like “WinMM” and “SslMM”, and their file naming spoofed MSN Talk and Msn Gaming Zone. The backdoor term “naikon” was derived from the User-Agent string “NOKIAN95”. But msnMM, naikon, sakto, and rarstone backdoors are all used by the same actor that we call the Naikon APT. Their second stage tools largely remained unknown, but a list is included in this report.

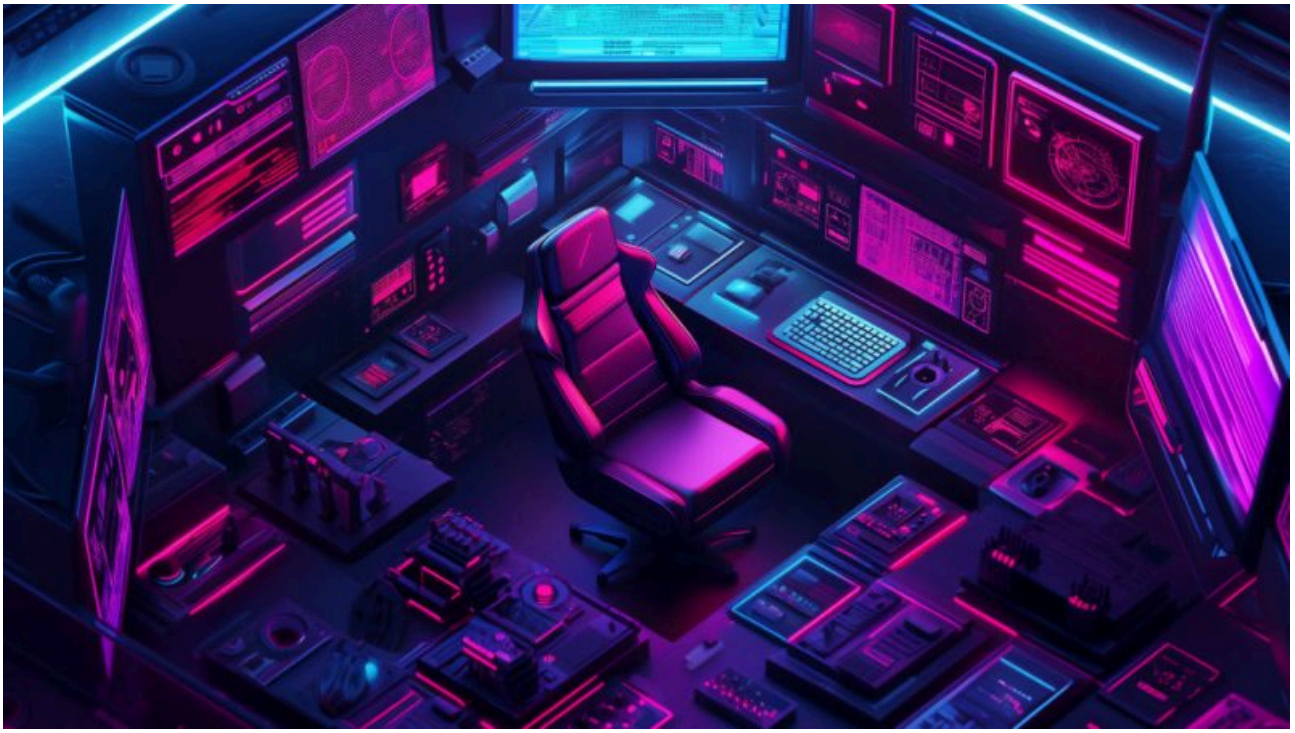
The Naikon attackers attempted to exfiltrate sensitive geo-political, military, and economic data; to intercept communications and to maintain surveillance on their victims throughout the MsnMM campaigns. Their toolset and techniques changed over time in many minor ways, and appear to be run by Chinese-speaking individuals. The group’s infrastructure, reliant on web apps located mostly via dynamic dns domains, overlapped across these campaigns. As previously described, the APT’s methods and technologies are simple, but highly effective against its targets’ defenses. We do not find 0-days here.

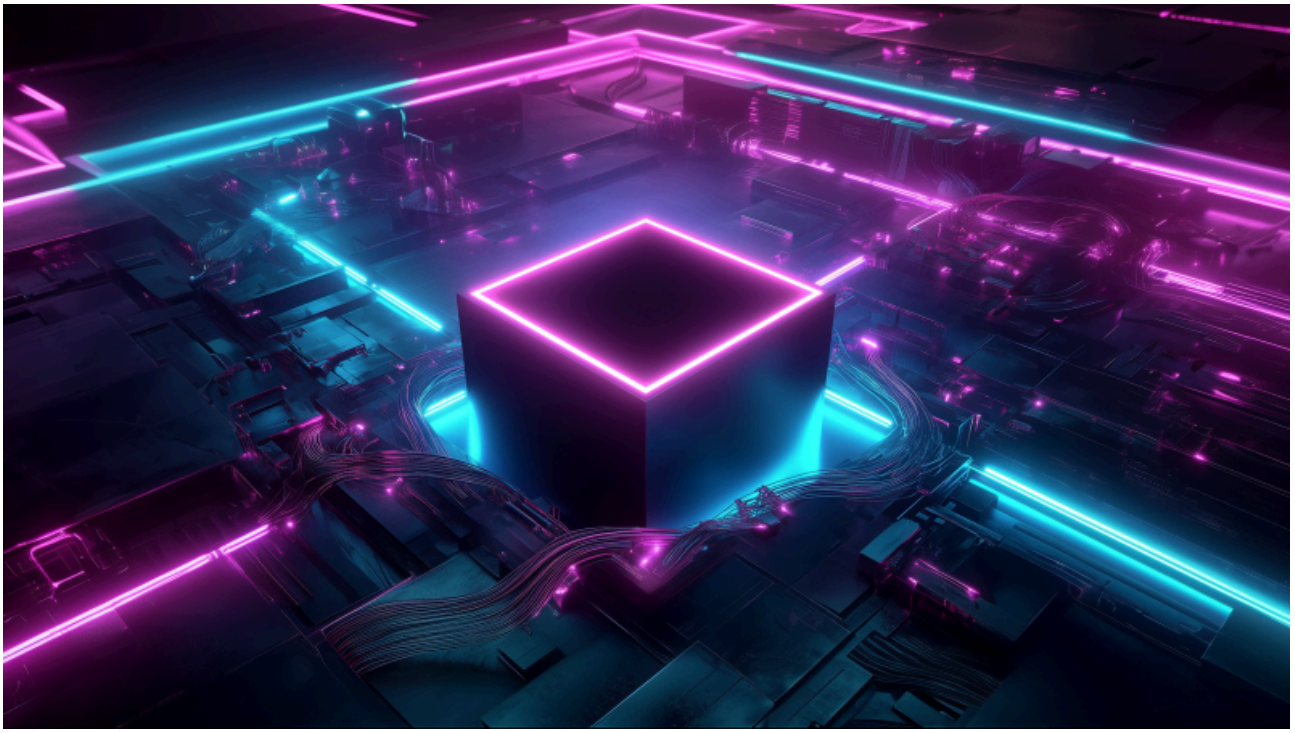
Much of Naikon’s spear-phish and decoy document content, as well as its deployment, coincided approximately with highly-charged geopolitical events. The consistent list of military, economic, and political targets gave away the actor’s interests. Naikon’s earliest campaigns deployed the exe_exchange, winMM, and sys10 backdoors, and the codebase was later built out into more custom tools. The MsnMM campaigns were waged into the start of 2014, and then dropped off before picking up again later in the year and into 2015.

Regarding interaction with other APTs, it's interesting to note that Naikon APT victims overlap with Cycldek APT victims. Cycldek is another persistent, but weaker APT. In addition, not only does the APT30 target profile match the Naikon APT, its toolset also features minor but noticeable similarities. And the later Naikon campaigns led to an all out APT v APT confrontation with the Hellsing APT, when "the empire struck back."

Although aspects of the malware set have been discussed on some blogs and in other papers, there hasn't been an accurate report bringing together details of the MsnMM, Sys10, and Naikon campaigns as the work of one crew, the Naikon APT. Finally, while this report looks into their past activity, the Naikon APT remains active, deploying a more recent codebase. The top targets for 2015 that we are aware of include organizations in Myanmar, Cambodia, Vietnam, Thailand, and Laos.

Latest Webinars





Reports

Kaspersky researchers analyze updated CoolClient backdoor and new tools and scripts used in HoneyMyte (aka Mustang Panda or Bronze President) APT campaigns, including three variants of a browser data stealer.

Kaspersky discloses a 2025 HoneyMyte (aka Mustang Panda or Bronze President) APT campaign, which uses a kernel-mode rootkit to deliver and protect a ToneShell backdoor.

Kaspersky GReAT experts analyze the Evasive Panda APT's infection chain, including shellcode encrypted with DPAPI and RC5, as well as the MgBot implant.

Kaspersky expert describes new malicious tools employed by the Cloud Atlas APT, including implants of their signature backdoors VBShower, VBCloud, PowerShower, and CloudAtlas.
