Sphinx Moth: Expanding our knowledge of the “Wild Neutron” / “Morpho” APT

research.kudelskisecurity.com/2015/11/05/sphinx-moth-expanding-our-knowledge-of-the-wild-neutron-morpho-apt/

kscert November 5, 2015

The Kudelski Security Cyber Fusion Center together with the KS-CERT has been monitoring and investigating the “Sphinx Moth” threat activity since mid-2014.

When Kaspersky and Symantec released reports on a powerful threat actor earlier this year, it became clear that what they had respectively called “Wild Neutron” or “Butterfly”/“Morpho”, corresponded with the “Sphinx Moth” advanced persistent threat that Kudelski Security was investigating as well.

Now that the threat actor has been exposed, we can expect them to change their Tactics, Techniques and Procedures (TTPs). We have decided to disclose several new Indicators of Compromise (IOCs) related to “Sphinx Moth” group with a view to furthering a collective understanding of the attack methods, tools and targets, and helping enterprises detect and eliminate any intrusion into their networks.

Attacks like “Sphinx Moth” are increasing. Yet despite their prevalence and our awareness about their impact, strategies to address the risk of cyberattacks remain inadequate. It is no longer possible to work on the assumption that we can fully protect a corporate network. With the rise of advanced persistent threats, enterprises can have an intruder in their network for months or years, without even being aware of its presence.

Key findings

Our report contains the analysis of 5 new binaries, and provides 5 new command and control server IP addresses, 2 new Command and Control domains, 6 new YARA rules, 1 new tactic to regain access and a Powershell script to detect the named pipes IOC on an SCCM infrastructure.

It’s available on the Kudelski Security website: Sphinx Moth Report