Cuckoo Spear – the latest Nation-state Threat Actor targeting Japanese companies

By Cybereason Security Services Team

Archived: 2026-04-05 20:39:06 UTC

Highly sophisticated, well-funded, and strategically motivated nation-state cybersecurity threats are complex and challenging, requiring advanced cybersecurity measures, threat intelligence, and international cooperation. Government agencies or state-sponsored groups, are engaging in cyber-attacks for various reasons, including espionage, sabotage, or for political influence.

Cuckoo Spear is the latest nation-state threat discovered through Cybereason threat analysis. By tying multiple incidents together, the report outlines how the associated Threat Actor persists stealthily on their victims' network for years. In fact Cybereason identified that the associated Threat Actor was present in victim networks for a time period between 2 and 3 years.

Disclosing new information about the APT10 group’s new arsenal and techniques, Cybereason highlights how defenders (organisations and governments) must implement robust security protocols, monitor for and detect suspicious activities, and collaborate with cybersecurity experts to mitigate the risks posed by such threats whilst preventing these attacks.

Since December 2019, the cybersecurity landscape has been continuously challenged by the emergence and evolution of the LODEINFO malware. Recent investigations suggest the involvement of a Chinese state-backed Advanced Persistent Threat (APT) group, likely APT10, in orchestrating these attacks. A recent development identified ties between the Threat Actor utilizing LODEINFO with a new malware family that is called NOOPDOOR. Cybereason named this threat Campaign “Cuckoo Spear”.

APT10 is a sophisticated Chinese state-sponsored cyber espionage group that has been active as early as 2006, according to the Department of Defense. The information security community widely believes the group's focus is to support Chinese national security goals by gathering intelligence against the relevant targets. APT10 often targets various critical infrastructure sectors such as communications, manufacturing and various public sectors.

Cuckoo Spear is related to the APT10 Intrusion Set because of the links made between various incidents from Threat Actors “Earth Kasha” (Trend Micro *) and “MirrorFace” including both APT10’s old arsenal (LODEINFO) and new arsenal identified in the Cybereason Threat Analysis Report. The actors behind NOOPDOOR not only utilized LODEINFO during the campaign, but also utilized the new backdoor to exfiltrate data from compromised enterprise networks. The intention behind this behaviour is likely espionage, as Threat Actors targeted critical infrastructure sectors and academic institutions, which are often intelligence gathering targets.

Techniques employed to load this highly sophisticated malware

In this recent Threat Analysis Report, Cybereason exhibits a new backdoor utilized by Threat Actors called NOOPDOOR, as dubbed by ESET and Trend Micro. NOOPDOOR is a 64-bit modular backdoor which employs DGA-based C2 communication. The backdoor is seen to be loaded by NOOPLDR, which is responsible for decrypting and executing NOOPDOOR.

Cybereason observed LODEINFO and NOOPLDR/NOOPDOOR (first known in January 2024) both in one case linking them together. As mentioned in different reports*, Threat Actors started to incorporate NOOPDOOR in the new campaigns. Based on the analysis of LODEINFO and as well as on the observation of these campaigns, LODEINFO appears to be used as a primary backdoor and NOOPDOOR acts as a secondary backdoor, keeping persistence within the compromised corporate network for more than two years.

Cybereason Research team Jin Ito, Incident Response Engineer, Loïc Castel, Incident Response Investigator, from the Cybereason IR Team and Kotaro Ogino, CTI Analyst, Cybereason Security Operations Team explored the sophisticated functionalities and tactics that define the most recent iteration of NOOPDOOR and NOOPLDR malware and its surrounding capabilities documenting in detail within the Threat Analysis Report.

A Sophisticated Set of Tools
During recent incident response activities, our team has uncovered and meticulously analyzed the newest arsenal deployed by the Threat Actor. This analysis, fueled by advanced reverse engineering techniques, revealed a sophisticated set of tools designed for stealth infiltration, data exfiltration, and persistent access.

A variety of different techniques were used to lure in potential victims, but the Threat Actors mainly rely on Spear-Phishing as the common initial access technique with LODEINFO; however, malicious actors have started to shift their tactics to exploiting vulnerabilities. NOOPDOOR must be loaded first on the victim machines, which is done through persistence mechanisms and Cybereason observed three different methods:

Scheduled Tasks: Threat Actors maintain persistence within the environment by abusing Scheduled Tasks. The scheduled task consists of execution of MSBuild, which loads malicious XML files and compiles the NOOPDOOR loader at runtime.

WMI Consumer Events: The Threat Actors leverage the WMI event consumer, which executes the main action when it gets triggered by a filter. The Threat actor then makes use of ActiveScript, which appears to execute in the JScript engine. For the consumer action in this WMI event, the Threat Actor leverages MSBuild execution for NOOPDOOR loader, similar to the scheduled task which also leverages MSBuild. Utilizing WMI event consumers are the alternate methodologies to persist within the environment.

Windows Services (Service DLL): Threat actors also maintain persistence within the environment by creating malicious services that load unsigned DLL files.

Detailed analysis on loading malicious code, and the reverse engineering of the Cuckoo Spear tools : NOOPLDR and NOOPDOOR are found in the Threat Analysis Report Arsenal Analysis chapter.

Strategies for Threat Hunting and Defense

Cybereason provided hunting queries to identify Cuckoo Spear presence in the network and has shared Indicators of Compromise (IOCs) within the Analysis Report to better detect them and potentially block Cuckoo Spear activity.

Due to the potential complexity of the containment, eradication and recovery process, it is highly recommended to hire a dedicated Incident Response team upon discovery of this Threat Actor being on the network.

In many APT related cases, the Threat Actor has already gained network access for several months or years before any investigation has started. Eradication of this Threat Actor requires in-depth preparation and effective security measures so the attacker cannot return. Although remediation actions will differ for each organization, Cybereason Security Services suggest, in general, to conduct an organization scale remediation day where the following actions are implemented:

- Prepare a clean uncompromised network
- Disabled all internet access to and from the internet
- Block all NOOPDOOR related C2 domains and IPs
- Reset all user passwords
- Rebuild infected machines
- Connect rebuilt machines to the clean network

Leveraging open-source intelligence, Cybereason provides actionable insights on how organizations can effectively hunt and defend against these persistent threats. If you have concerns about nation-state level threats or need advice on how to protect against them, feel free to ask Cybereason for more specific information.

For detailed Analysis, hunting queries and scripting, read the latest Cybereason Threat Report now.

*Trend Micro and ESET research findings JSAC2024
