# Kaspersky discovers poorly detected backdoor, targeting governments and NGOs around the globe

By Kaspersky

Published: 2022-06-30 · Archived: 2026-04-05 22:28:38 UTC

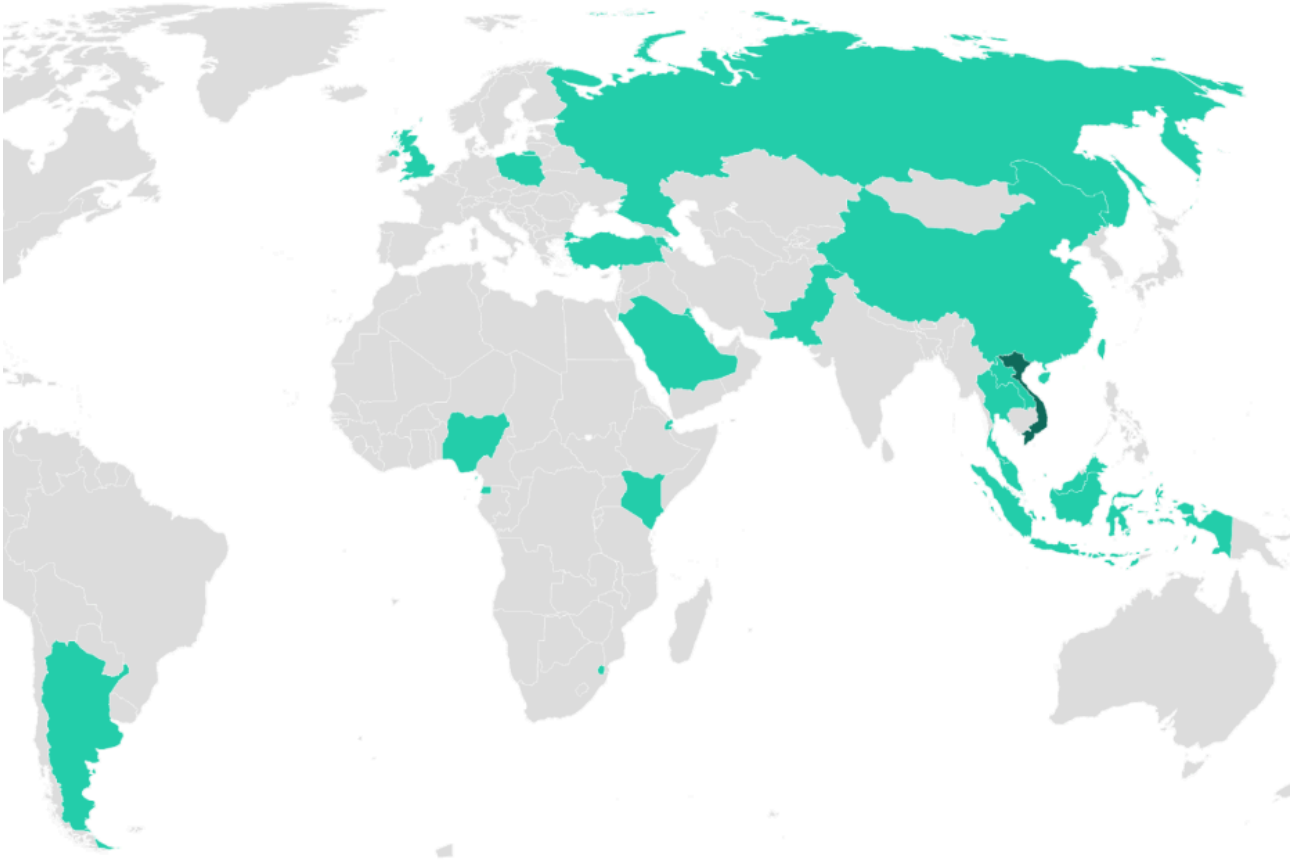
**Kaspersky experts have brought to light a poorly detected SessionManager backdoor that was set up as a malicious module within the Internet Information Services (IIS), a popular web server edited by Microsoft. Once propagated, SessionManager enables a wide range of malicious activities, starting from collecting emails to complete control over the victim's infrastructure. First leveraged in late March 2021, the newly discovered backdoor has hit governmental institutions and NGOs in Africa, South Asia, Europe and the Middle East. Most of the targeted organizations are still compromised to date.**

In December 2021, Kaspersky uncovered "Owowa", a previously unknown IIS module that steals credentials entered by a user when logging into Outlook Web Access (OWA). Since then, the company's experts have kept an eye on the new opportunity for cybercriminal activity – it has become clear that deploying a backdoor within IIS is a trend for threat actors, who previously exploited one of the "ProxyLogon-type" vulnerabilities within Microsoft Exchange servers. In a recent investigation, Kaspersky experts came across a new unwanted module backdoor, dubbed SessionManager.

The SessionManager backdoor enables threat actors to keep persistent, update-resistant and rather stealth access to the IT infrastructure of a targeted organization. Once dropped into the victim's system, cybercriminals behind the backdoor can gain access to company emails, update further malicious access by installing other types of malware or clandestinely manage compromised servers, which can be leveraged as malicious infrastructure.

A distinctive feature of SessionManager is its poor detection rate. First discovered by Kaspersky researchers in early 2022, some of the backdoor samples were still not flagged as malicious in most popular online file scanning services. To date, SessionManager is still deployed in more than 90% of targeted organizations according to an Internet scan carried out by Kaspersky researchers.

Overall, 34 servers of 24 organizations from Europe, the Middle East, South Asia and Africa were compromised by SessionManager. The threat actor who operates SessionManager shows a special interest in NGOs and government entities, but medical organizations, oil companies, transportation companies, among others, have been targeted as well.



*Map of organizations targeted by SessionManager campaign*

Because of a similar victimology and the use of the common "OwlProxy" variant, Kaspersky experts believe that the malicious IIS module might have been leveraged by the GELSEMIUM threat actor, as part of its espionage operations.

*"The exploitation of exchange server vulnerabilities has been a favorite of cybercriminals looking to get into targeted infrastructure since Q1 2021. It notably enabled a series of long unnoticed cyberespionage campaigns. The recently discovered SessionManager was poorly detected for a year and is still deployed in the wild. Facing massive and unprecedented server-side vulnerability exploitation, most cybersecurity actors were busy investigating and responding to the first identified offences. As a result, it is still possible to discover related malicious activities months or years later, and this will probably be the case for a long time,"* comments Pierre Delcher, Senior Security Researcher at Kaspersky's Global Research and Analysis team.

*"Gaining visibility into actual and recent cyberthreats is paramount for companies to protect their assets. Such attacks may result in significant financial or reputational losses and may disrupt a target's operations. Threat intelligence is the only component that can enable reliable and timely anticipation of such threats. In the case of Exchange servers, we cannot stress it enough: the past-year's vulnerabilities have made them perfect targets, whatever the malicious intent, so they should be carefully audited and monitored for hidden implants, if they were not already,"* adds Pierre.

Kaspersky products detect several malicious IIS modules, including SessionManager. To learn more about SessionManager's operation style and targets, visit Securelist.com.

To protect your businesses from such threats, Kaspersky experts also recommend that you:

- Regularly check loaded IIS modules on exposed IIS servers (notably Exchange servers), leveraging existing tools from the IIS servers suite. Check for such modules as part of your threat hunting activities every time a major vulnerability is announced on Microsoft server products.
- Focus your defense strategy on detecting lateral movements and data exfiltration to the internet. Pay special attention to outgoing traffic to detect cybercriminal connections. Back up data regularly. Make sure you can quickly access it in an emergency.
- Use solutions like Kaspersky Endpoint Detection and Response and the Kaspersky Managed Detection and Response service, which help to identify and stop the attack in the early stages, before the attackers achieve their goals.
- Use a reliable endpoint security solution, such as Kaspersky Endpoint Security for Business (KESB) that is powered by exploit prevention, behavior detection and a remediation engine that is able to roll back malicious actions. KESB also has self-defense mechanisms that can prevent its removal by cybercriminals.

**About Kaspersky**

Kaspersky is a global cybersecurity and digital privacy company founded in 1997. Kaspersky's deep threat intelligence and security expertise is constantly transforming into innovative security solutions and services to protect businesses, critical infrastructure, governments and consumers around the globe. The company's comprehensive security portfolio includes leading endpoint protection and a number of specialized security solutions and services to fight sophisticated and evolving digital threats. Over 400 million users are protected by Kaspersky technologies and we help 240,000 corporate clients protect what matters most to them. Learn more at www.kaspersky.com.

---