GhostEmperor: Chinese-speaking APT targets high-profile victims using unknown rootkit

By Kaspersky

Published: 2021-07-29 · Archived: 2026-04-05 22:28:13 UTC

According to Kaspersky's quarterly report, the threat landscape saw an increase in attacks against Microsoft Exchange servers in Q2 2021. In the latest APT 2021 Report, Kaspersky reveals the details of a unique long-standing operation, 'GhostEmperor', which uses Microsoft Exchange vulnerabilities to target high-profile victims with an advanced toolset and no affinity to any known threat actor.

Advanced persistent threat (APT) actors are constantly seeking new, more sophisticated ways to perform their attacks. That is why Kaspersky researchers monitor how APT groups refresh and update their toolsets. According to Kaspersky's quarterly report, the threat landscape saw an increase in attacks against Microsoft Exchange servers in Q2 2021. In the latest APT 2021 Report, Kaspersky reveals the details of a unique long-standing operation, 'GhostEmperor', which uses Microsoft Exchange vulnerabilities to target high-profile victims with an advanced toolset and no affinity to any known threat actor.

GhostEmperor is a Chinese-speaking threat actor that has been discovered by Kaspersky researchers. It mostly focuses on targets in Southeast Asia, including several governmental entities and telecoms companies.

This actor stands out because it uses a formerly unknown Windows kernel-mode rootkit. Rootkits provide remote control access over the servers they target. Acting covertly, rootkits are notorious for hiding from investigators and security solutions. To bypass the Windows Driver Signature Enforcement mechanism, GhostEmperor uses a loading scheme involving the component of an open-source project named "Cheat Engine". This advanced toolset is unique and Kaspersky researchers see no affinity to already known threat actors. Kaspersky experts have surmised that this toolset has been in use since at least July 2020.

"As detection and protection techniques evolve, so do APT actors. They typically refresh and update their toolsets. GhostEmperor is a clear example of how cybercriminals look for new techniques to use and new vulnerabilities to exploit. Using a previously unknown, sophisticated rootkit, they brought new problems to the already well-established trend of attacks against Microsoft Exchange servers," comments David Emm, security expert at Kaspersky.

Besides the growth of attacks against Microsoft Exchange servers, Kaspersky experts also highlight the following trends on the APT landscape in Q2:

- There has been a rise in APT threat actors leveraging exploits to gain an initial foothold in attacked networks – including the zero-days developed by the exploit developer 'Moses' and those used in the PuzzleMaker, Pulse Secure attacks, and the Microsoft Exchange server vulnerabilities
- APT threat actors continue to invest in refreshing their toolsets: this includes not only the inclusion of new platforms but also the use of additional languages, as seen by WildPressure's macOS-supported Python

malware
- While some of the supply-chain attacks were major and have attracted worldwide attention, Kaspersky experts also observed equally successful low-tech attacks, such as BountyGlad, CoughingDown, and the attack targeting Codecov, which signaled that low-key campaigns still represent a significant threat to security

To learn more about GhostEmperor and other significant discoveries of the quarter, read the APT trends report Q2 2021 on Securelist. The report summarizes the findings of Kaspersky's subscriber-only threat intelligence reports, which also include Indicators of Compromise (IoC) data and YARA rules to assist in forensics and malware hunting. For more information, please contact: intelreports@kaspersky.com

In order to avoid falling victim to a targeted attack by a known or unknown threat actor, Kaspersky researchers recommend implementing the following measures:

- Provide your SOC team with access to the latest threat intelligence (TI). The Kaspersky Threat Intelligence Portal is a single point of access for the company's TI, providing cyberattack data and insights gathered by Kaspersky spanning over 20 years. Free access to its curated features that allow users to check files, URLs, and IP addresses, are available here
- Upskill your cybersecurity team to tackle the latest targeted threats with Kaspersky online training developed by GReAT experts
- For endpoint level detection, investigation, and timely remediation of incidents, implement EDR solutions such as Kaspersky Endpoint Detection and Response
- In addition to adopting essential endpoint protection, implement a corporate-grade security solution that detects advanced threats on the network level at an early stage, such as Kaspersky Anti Targeted Attack Platform
- As many targeted attacks start with phishing or other social engineering techniques, introduce security awareness training and teach practical skills to your team – for example, through the Kaspersky Automated Security Awareness Platform

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.
