# GhostEmperor returns with updated Demodex rootkit

Original report published on: July 17, 2024[1]

## Executive Summary

GhostEmperor, a Chinese-nexus threat group targeting primarily South-East Asian telecommunication and government entities updated their Demodex rootkit to evade Endpoint Detection & Response (EDR) detection, impede sandbox analysis, and use reflective loader to run in memory to deploy Demodex.

## Background

GhostEmperor is a Chinese-nexus threat group, first identified by Kaspersky in 2021 and known to target mostly South-East Asian telecommunications and government entities. In 2021, they gained initial access through exploiting vulnerabilities in public-facing servers such as Microsoft Exchange and used ProxyLogon vulnerability to gain access and perform remote code execution.[2]

Once initial access was obtained, WMIExec (Impacket, a popular tool used by red teams and threat actors) was used to remotely execute a batch file. The batch file executed built-in Windows tools to extract and import files where one of the extracted files was a Powershell script that creates a malicious service DLL that masquerades a legitimate Windows system process to avoid detection. The service DLL was then used to install Demodex rootkit.

The updated Demodex rootkit uses legitimate Windows tools more extensively to avoid detection, has enhanced EDR evasion capabilities, anti-user-mode hooking to impede analysis, and uses reflective loader (loading DLL in memory) to execute the Core-Implant. The Core-Implant which was used to manage Command and Control (C2) communication and install Demodex rootkit had to bypass the Driver Signature Enforcement (DSE) security feature, which blocks unsigned drivers. To bypass DSE, 'Cheat Engine' – an open-source tool used for video game cheating was used to manipulate memory and execute code in kernel space to install Demodex.

## Detection and Mitigation

IMDA recommends organisations to perform continual testing and validating of existing security controls to ensure detection and prevention against the MITRE ATT&CK techniques identified in this advisory:

- Refer to the MITRE ATT&CK techniques in this advisory:
  - Create, test and validate detection rules against the threat behaviours.
  - Validate and deny/disable processes, ports and protocols that have no business need.
- Validate and add malicious file hashes to blocklist in anti-virus and/or Endpoint Detection & Response (EDR) and eXtended Detection and Response (XDR).
- Implement the principle of least privilege by restricting access to sensitive data and closely monitoring user permissions to make it more challenging for attackers to move laterally.
- Keep all public facing systems updated with the latest security patch.
- Set execution policies to 'AllSigned' to require all Powershell scripts, whether local or remote, to be signed by a trusted publisher to run.
- Deploy data loss prevention (DLP) solution to monitor and block unauthorised data exfiltration.

IMDA encourages organisations to conduct thorough analysis to identify potential risks and assess their potential impact prior to deploying defensive measures.

## Indicators of Compromise

| Malware Hashes – SHA1 | Remarks |
|---|---|
| 43f1c44fa14f9ce2c0ba9451de2f7d3dd1a208de | prints1m.dll |
| a59cca28205eeb94c331010060f86ad2f3d41882 | service.ps1 |
| bab2ae2788dee2c41065850b2877202e57369f37 | dbk64.sys |

| Domain | Remarks |
|---|---|
| imap.dateupdata[.]com | C2 |

| IP Address | Remarks |
|---|---|
| 193[.]239[.]86[.]168 | C2 |

## MITRE ATT&CK Tactics and Techniques

| Tactic | Technique ID | Technique Name |
|---|---|---|
| Initial Access | T1190 | Exploit Public-Facing Application |
| Execution | T1059.001 | Command and Scripting Interpreter: Powershell |
| | T1059.003 | Command and Scripting Interpreter: Windows Command Shell |
| | T1047 | Windows Management Instrument |
| | T1069.002 | System Service: Service Execution |
| Privilege Escalation | T1068 | Exploitation for Privilege Escalation |
| Defense Evasion | T1014 | Rootkit |
| | T1620 | Reflective Code Loading |
| | T1027 | Obfuscated Files or Information |
| | T1140 | Deobfuscate/Decode File or Information |
| | T1036.004 | Masquerading: Masquerading Task and Service |
| | T1112 | Modify Registry |
| Credential Access | T1003 | OS Credential Dumping |

| | | |
|---|---|---|
| Discovery | T1049 | System Network Connections Discovery |
| Lateral Movement | T1021 | Remote Services |
| Collection | T1005 | Data from Local System |
| Command and Control | T1071 | Application Layer Protocol |
| Exfiltration | T1041 | Exfiltration Over C2 Channel |

## References


1. **^** "The Return of GhostEmperor's Demodex".
2. **^** "GhostEmperor: From ProxyLogon to kernel mode".