

Guloader Malware Being Disguised as Employee Performance Reports

A asec.ahnlab.com/en/91825

ATCP

January 8, 2026



AhnLab SEcurity intelligence Center (ASEC) recently discovered the Guloader malware being distributed via phishing emails disguised as an employee performance report. The email claims to be informing the recipient about the report for October 2025, and prompts the recipient to check the attachment by mentioning the plan to dismiss some employees.



Figure 1. Phishing email body

The attached file is a compressed file in RAR format, and it contains an NSIS executable file named “staff record pdf.exe” inside. If the extension is not displayed, there is a risk of being mistaken for a PDF document and being executed, so please be cautious.



Figure 2. Inside the attached compressed file

The staff record pdf.exe file is Guloader malware. When executed, it loads and executes the shellcode located in the C2 below into memory.

URL : <https://drive.google.com/uc?export=download&id=1bzvByYrIH24oMCIX7Cv41gP9ZY3pRsgv>



Figure 3. Shellcode being downloaded

The final malware that is executed is Remcos RAT. It allows threat actors to perform malicious remote control behaviors such as keylogging, capturing screenshots, controlling webcams and microphones, as well as extracting browser histories and passwords from the installed system.

Remcos RAT C2 : 196.251.116[.]219:2404,5000



Figure 4. C2 information of Remcos RAT

Users must be extra cautious when opening emails from unknown sources. Regular password changes are necessary to prevent secondary damage. Additionally, unlike cases where threat actors use their own address or breached addresses to leak information, the number of cases where normal platforms are used as C2 is continuously increasing, so users must be extra cautious.

MD5

c95f2a7556902302f352c97b7eed4159

Gain access to related IOCs and detailed analysis by subscribing to **AhnLab TIP**. For subscription details, click the banner below.



AhnLab TIP

Stay Ahead of Rapidly Evolving Threats Make the Best-Informed Decisions

Get Started with AhnLab's State-of-the-Art Threat Intelligence

atip.ahnlab.com