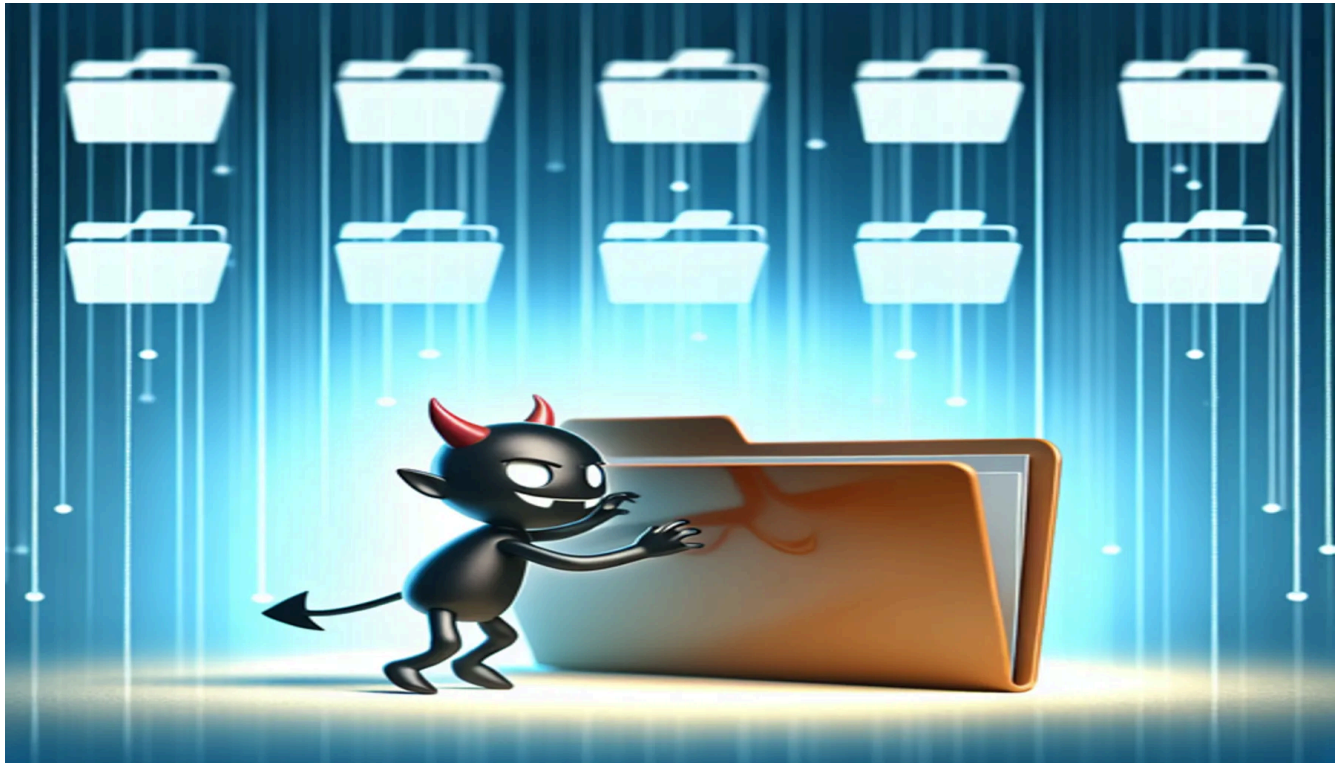


April 2026 Security Issues in Korean & Global Financial Sector

A asec.ahnlab.com/en/93805

ATCP

May 12, 2026



Statistics on Malware Distributed to the Financial Sector

attack Stage 1 Phishing, Attack Stage 2 Backdoor-Downloader-Dropper, and Attack Stage 3 Infostealer-Ransomware were identified as the top malware in the financial sector. The actual distribution files were identified based on MD5 Hash, and it was explained that there may be many variants of the same family.

Top 10 Major Malware Strains Distributed to the Financial Sector

the Korean file names used in the phishing and malware distribution include RFQ-097970-H2551-N0-20897--**0976-order.bat**, -송금내역NoticeSecure.htm, 단가인상문--**260413-1.pdf, RemittanceDetailedInformationSecure.htm, RemittanceResultInformationEncrypted.htm, and Resume260407I will be a candidate who is sincere and consistent in all things.exe. the threat actors disguised them as work documents, tax and payment proofs, and HR and contract documents to induce trust.

Statistics on accounts of Korean industries exfiltrated via Telegram

malware information collected through malware and phishing emails in Korea was leaked to attackers through Telegram API. phishing emails with keywords such as remittance, receipt, voicemail, malicious links, and HTML files were sent to the login page, and the entered account ID and password were sent to the threat actor's Telegram chat room. the report said the quantity of accounts from Korea's financial sector that were compromised via Telegram during January accounted for 2 percent of the total.

Major Deep Web & Dark Web Issues in the Financial Sector

KISA announced a RCE (Remote Code Execution) vulnerability in WGear, a corporate banking e-finance software from Inswave. The vulnerability occurs in WGear version 1.100.7.0205 and earlier, and allows threat actors to remotely execute arbitrary code. in a real-world example, a WGear process executed mshta to call external HTML, which then downloaded and executed additional payloads and finally installed GeniexLoader. this vulnerability has been consistently exploited by Andariel, and GeniexLoader` has been linked to BlueNoroff (a.k.a CryptoCore, APT38).

database leaks, account information sales, and access sales have been observed on the dark web and cybercrime forums. the ShinyHunters' on BreachForums' attempted to sell Santander Bank customer Data for approximately \$1 million, claiming to have more than 30 million customers, more than 6 million account information and balances, and more than 28 million credit card numbers. secur3rat on DarkForums claimed to sell approximately 26,554 Deutsche Bank-related combo lists for \$200, but the sample included many unrelated and generic website addresses. on BreachForums, RubiconH4ck` claimed to have a Brazilian financial Data set of approximately 2.3 million hits, including Banco do Brasil.

other confirmed ransomware releases include Everest, Prinz Eugen and Qilin. everest posted Citizens Bank as a victim and claimed to have Data and internal table information from approximately 3.4 million transactions, with a countdown end date of April 28, 2026. Prinz Eugen claimed that 1.2 TB and more than 154 million SQL Data were taken from Standard Bank and released the files in phases of PUBLICATION. qilin posted Manulife Wealth & Asset Management as a victim, but the specific size of the breach was not confirmed.

the sale of access was also observed. root-level access to the Linux-based firewall of a large US-based Financial services firm was sold for \$400, while access to the core API of a global

financial transaction firm was offered for \$80,000 in Monero. insecure Direct Object Reference (IDOR) access to a Latin American financial firm was also sold for \$10,000, claiming access to approximately 2 million customers' Data. such instances can lead to Data breaches, ransomware infections, and financial fraud, and require constant monitoring.

MD5

15adac4d6fc1bddb0c940cdc0c6605b4

53636c80d43a3c461dc8a3d2a2f2d4e1

750173f1b36e502ff17e2c5eec03c602

8edc77fb36bf80bb52d158cf9043cecd

b15a55f9a23998b1976622bd3b9a3ad9

Additional IOCs are available on AhnLab TIP.