TA505 hacking crew spent much of 2019 trying to breach South Korea's financial sector

By Jeff Stone

Published: 2020-02-28 · Archived: 2026-04-05 16:53:39 UTC

A gang of hackers with a long history of financially motivated attacks increased its targeting of businesses in South Korea last year, using a combination of malicious attachments and ransomware to haunt victims, according to new findings.

Researchers from the Financial Security Institute, which is similar to an information sharing and analysis center (ISAC) for South Korea's financial sector, said on Friday that the hacking group spent much of 2019 trying to phish enterprises in finance, manufacturing and medical services in South Korea.

The group, known as TA505, has been active since at least 2014, and appears to share tools, techniques and procedures with FIN7, a Russian-speaking group blamed for more than a billion dollars in global losses, researchers say. Linking FIN7 and TA505 is a notoriously difficult task, and researchers have confused the groups before.

TA505 is perhaps best known for its reported connection to the Dridex banking trojan, which enables attackers to steal banking credentials, and the Locky ransomware strain, which has targeted victims since 2016. Like FIN7, TA505 also is a Russian-speaking group, according to previous reports, and previously sent thousands of malicious emails to bank employees in the U.S., United Arab Emirates and Singapore, email security firm Proofpoint said last year.

The Financial Security Institute said Friday that many of the phishing emails TA505 sent throughout South Korea included malicious Microsoft Excel documents, and often relied on the "FlawedAmmyy" malware. FlawedAmmyy is a remote access trojan, meaning it gives attackers control over an infected machine without a victim's knowledge. From there, they can monitor a user's activity and collect their usernames and passwords.

The analysis of 612,021 phishing emails from between February and December last year showed that 81% of the messages were sent on weekdays, mostly Thursday (25.7%) and Wednesday (24.5%). For researchers, the timing "indicates that the group figures out the most vulnerable time slot of Korean users." They also found a phishing page which masqueraded as an Apple log-in portal, an apparent indication that TA505 also aimed to steal data from Korean customers of the U.S. technology company.

TA505 also used a ransomware strain called Rapid, a new technique for the group, according to the Financial Security Institute. "Rapid" appeared in just one case, which also involved a malicious Excel file. "This can be [a] one-short time use of Rapid ransomware," researchers wrote. "But we need to keep track of it in case they use it for a longer campaign."

CyberScoop has independently verified the Financial Security Institute's findings with external researchers.

Source: https://www.cyberscoop.com/ta505-south-korea-bank-phishing/